FAULT DIAGNOSIS AND FAULT-TOLERANT CONTROL OF CHEMICAL PROCESS SYSTEMS

FAULT DIAGNOSIS AND FAULT-TOLERANT CONTROL OF CHEMICAL PROCESS SYSTEMS

By Miao Du, B. Eng., M. Information Science and Technology

A Thesis Submitted to the School of Graduate Studies

in Partial Fulfilment of the Requirements

for the Degree of

Doctor of Philosophy

McMaster University Doctor of Philosophy (2012) Hamilton, Ontario (Chemical Engineering)

TITLE: Fault Diagnosis and Fault-Tolerant Control of Chemical Process Systems AUTHOR: Miao Du, B. Eng. (Zhejiang University), M. Information Science and Technology (Hokkaido University) SUPERVISOR: Dr. Prashant Mhaskar NUMBER OF PAGES: xviii, 176

Abstract

This thesis considers the problem of fault diagnosis and fault-tolerant control (FTC) for chemical process systems with nonlinear dynamics. The primary objective of fault diagnosis discussed in this work is to identify the failed actuator or sensor by using the information embodied in a process model, as well as input and output data. To this end, an active fault isolation method is first proposed to identify actuator faults and process disturbances by utilizing control action and process nonlinearity. The key idea is to move the process to a region upon fault detection where the effect of each fault can be differentiated from others. The proposed method enables isolation of faults that may not be achievable under nominal operation. This work then investigates the problem of sensor fault isolation by exploiting model-based sensor redundancy through state observer design. Specifically, a high-gain observer is presented and the stability property of the closed-loop system is rigorously established. A method that uses a bank of high-gain observers is then proposed to isolate sensor faults, which explicitly accounts for process nonlinearity, and to continue nominal operation upon fault isolation. In addition to fault diagnosis, this work addresses the problem of handling severe actuator faults using a safe-parking approach and integrating fault diagnosis and safe-parking techniques in a unified fault-handling framework. In particular, several practical issues are considered for the design and implementation of safe-parking techniques, including changes in process dynamics, the network structure of a chemical plant, and actuators frozen at arbitrary positions. The advantage of this approach is that it enables stable process operation under faulty conditions, avoiding the partial or entire shutdown of a chemical plant and resulting economic losses. The efficacy of the proposed fault diagnosis and FTC methods is demonstrated through numerous simulations of chemical process examples.

Acknowledgments

I would like to thank Dr. Prashant Mhaskar for giving me the opportunity to study in the Department of Chemical Engineering at McMaster University. His encouragement, guidance, and instructions are the key ingredients for the derivation of the results presented in this thesis. During this period of time, I have learned a number of skills regarding how to carry out scientific research independently and through team work in the field of engineering. I will definitely benefit from this wonderful experience in the future career. I would like to thank Dr. Benoit Chachuat, Dr. Tim Davidson, Dr. Thomas A. Adams II, and Dr. Jie Yu for their service on my supervisory committee. The discussions at committee meetings have led to thinking from different perspectives, improved the way that the results are presented, and corrected technical inaccuracies. I would like to thank the anonymous reviewers for their insightful comments, which have significantly enriched the results of this work and improved the quality of the results presented in this thesis. I would also like to thank the Department of Chemical Engineering for the fundamental graduate courses and McMaster Advanced Control Consortium (MACC) for the opportunities to interact with industrial representatives. Finally, I would like to thank my parents for their constant material and spiritual support.

Miao Du
Hamilton, Ontario
September, 2012

To my dear parents

Contents

List of Figures

List of Tables

List of Symbols and Acronyms

Symbols

n	vector size
$\equiv$	identically equal
$:=$	defined as
$<$ $(>)$	less (greater) than
$\leq$ $(\geq)$	less (greater) than or equal to
$\forall$	for all
$\in$	belongs to
$\subset$	subset of or equal to
$\rightarrow$	tends to or goes to
$\sum$	summation
$\|a\|$	the absolute value of a scalar a
$\|\|x\|\|$	the norm of a vector x
max	maximum
min	minimum
$f : S_1 \rightarrow S_2$	a function f mapping a set S_1 into a set S_2
$L_f h$	the Lie derivative of h with respect to the vector field f
blockdiag$[A_1, \ldots, A_n]$	a block diagonal matrix with diagonal blocks A_1 to A_n
$\lambda_{\max}(P)(\lambda_{\min}(P))$	the maximum (minimum) eigenvalue of a symmetric matrix P
$\mathrm{sgn}(\cdot)$	the signum function
$\square$	designation of the end of proofs
$\varnothing$	empty set
$\mathbb{R}^n$	the n-dimensional Euclidian space
lim sup	supremum limit
$D(\cdot)$	the fault distribution matrix
x	vector of state variables
u	vector of input variables
y	vector of output variables

$\hat{x}$	vector of state estimates
x_{nom}	system state at the nominal equilibrium point
x_s	system state at a safe-park point
t_f	fault occurrence time
t_r	fault repair time
t_d	time of fault detection
$\tilde{u}$	actuator faults
$\tilde{p}$	process faults
$\tilde{y}$	sensor faults
r	residual
t_h	threshold
V	Lyapunov function
Ω	stability region
Π	feasibility region
B_d	ball of radius d

Acronyms

FDD	fault detection and diagnosis
CLF	control Lyapunov function
CSTR	continuous-stirred tank reactor
FDI	fault detection and isolation
FTC	fault-tolerant control
LQ	linear-quadratic
MMA	methyl methacrylate
MPC	model predictive control
PCA	principal component analysis
PLS	partial least squares
SPE	squared prediction error
VAc	vinyl acetate

Chapter 1

Introduction

1.1 Motivation

The last few decades have witnessed significant improvements in efficiency and profitability of chemical process operations due to the advances in automatic control techniques. For example, model predictive control (MPC) has been extensively studied using a variety of approaches since the 1980s [1]. Nowadays, numerous chemical plants are benefiting from this control strategy that is able to effectively deal with multivariate constrained control problems. The increased level of automation, however, also makes process control systems susceptible to equipment abnormalities, such as failures in actuators (e.g., valves and pumps) or sensors (e.g., thermocouples, flow meters, and gas chromatographs). If not properly handled, they can lead to consequences ranging from failures to meet product quality specifications to plant shutdowns, incurring substantial economic losses, and even safety hazards to facilities and personnel, as well as damages to the environment. For instance, the U.S. petrochemical industry loses an estimated $20 billion per year because of abnormalities at oil refineries and chemical plants [2]. This implies that the traditional process control design, where the objective is to stabilize a process at a desired operating point in the absence of faults, is insufficient to ensure lasting optimal process operations. Therefore, it becomes increasingly important and necessary to take into account the problem of dealing with faults in the design of process control systems. This realization strongly motivates researchers and engineers to develop systemic, practically implementable, and automated techniques for the better handling of faults.

As with control designs, the complexities of chemical process systems pose several challenges to the handling of faults. Above all, most chemical processes exhibit nonlinear dynamics. A representative source of nonlinearity is the temperature dependence of the specific reaction rate as described by the Arrhenius equation. This invalidates the results developed for linear systems or linear approximations of nonlinear systems. Second, a common situation in a chemical plant is that not all the process states are measured due to economic considerations and the unavailability of effective sensors. The unavailability of full state measurements adds another layer of complexity to the problem of fault-handling. Third, an important feature of chemical processes is the intricate interconnection of spatially distributed units via a network of material and energy streams. Different from handling faults in an isolated unit, the effect of a fault taking place in one unit on the other units in the network should be accounted for in the fault-handling mechanism design. Finally, faults have multiplicity, such as the location in a closed-loop control system and its time-varying behavior. This characteristic asks for dedicated fault-handling designs for different faulty scenarios. While there is a significant body of results developed for linear systems and certain classes of nonlinear systems and faults, there does not exist a universal approach that can address all the complexities and meet the increasingly emerging demands from engineering practice. Motivated by the above, this thesis considers the problem of fault diagnosis and fault-tolerant control (FTC) for chemical process systems and addresses the aforementioned challenges by proposing novel methods and designs.

1.2 Background

A fault is an unpermitted deviation of input, output, or parameter of the system from the usual conditions. According to the location of the occurrence, faults can be categorized into actuator faults, sensor faults, and process faults, as shown in Fig. 1.1. Actuator faults can take place due to reasons such as mechanical failures and losses of power. Typically, an actuator works in a way that upon the occurrence of a complete failure, it reverts to shut (see Fig. 1.2(a)) or complete open (see Fig. 1.2(b)) to avoid hazardous situations, or it freezes to avoid introducing abrupt perturbations to the process (see Fig. 1.2(c)). This shut or complete open position is termed a fail-safe position. In the presence of actuator faults, the superior performance of a well designed control law would be directly jeopardized because the prescribed control action cannot be implemented in an expected way. In addition to actuators, sensors are another set of key components forming a feedback control loop. Sensor faults can take place due to reasons such as sensing component degradations, short circuits, and incorrect calibrations. In the presence of sensor faults, the controller will gen-

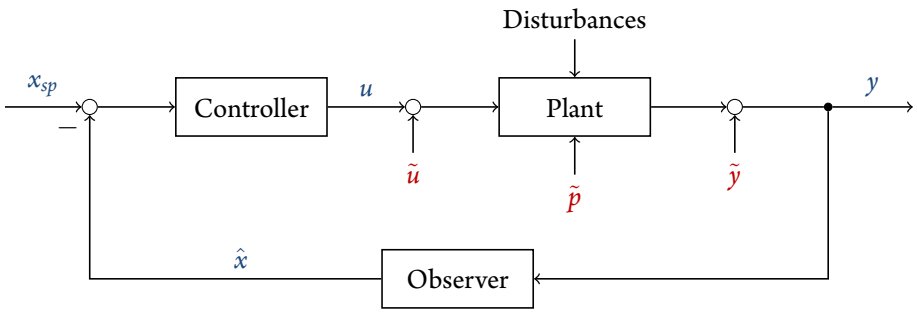

Figure 1.1: A process control system subject to faults. The control objective under normal conditions is to stabilize the process at a set point x_{sp} in the presence of disturbances. The measured output y is used to generate a state estimate $\hat{x}$, which is then used to compute a control input u through a feedback control law. The notations $\tilde{u}$, $\tilde{y}$, and $\tilde{p}$, denote actuator, sensor, and process faults, respectively.

erate incorrect or undesired control action. While the prescribed control action can be implemented to the process, the controller typically fails to stabilize the process at the optimal operating point, leading to off-spec production. Process faults are the third type of abnormalities, which include significant process disturbances and drifts in process parameters. They can take place due to perturbations from other parts of a plant, coking, deactivation of catalyst, and so on. According to the time-varying behaviors, faults can be categorized into persistent faults and intermittent faults. Persistent faults include complete failures and bias or drift faults. Intermittent faults are usually discussed in the context of networked control systems, where a data network is used as feedback media. Due to communication congestions between a controller and sensors or actuators, updated measurements or control inputs become unavailable intermittently.

The handling of faults includes three tasks: fault detection, fault diagnosis, and FTC. The objective of fault detection is to detect the occurrence of an abnormality as early as possible. The primary objective of fault diagnosis is to identify the faulty equipment (i.e., the location of a fault). Determining the location of a fault is termed fault isolation[1]. Besides isolating faults, fault diagnosis also includes estimating the size of the fault or determining its time-varying behavior [3]. Detecting and isolating a fault is termed fault detection and isolation (FDI). After a fault is detected and isolated, an FTC strategy can be used to minimize the effect of faults. The design of FTC strategies often includes a nonlinear control design and a fault-handling mechanism design, such as a supervisory control law.

According to the sources of the knowledge about the process, the existing results

[1]In literature, fault diagnosis and fault isolation are often used interchangeably if it does not cause any ambiguity.

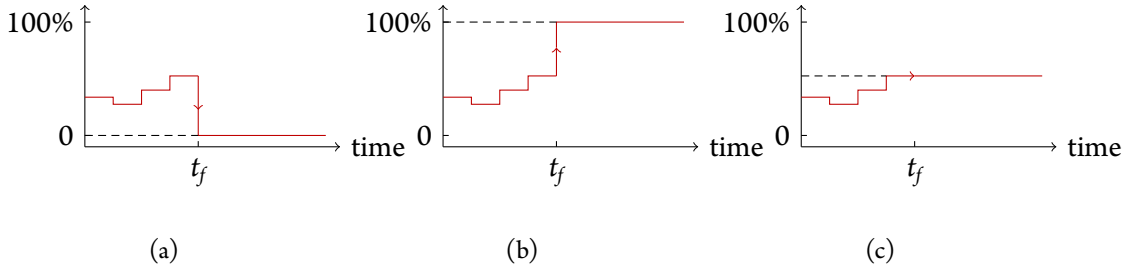

Figure 1.2: Illustration of the action of a failed actuator when a fault takes place at time t_f. (a) An actuator (e.g., used to control the fuel flow rate) reverts to shut position. (b) An actuator (e.g., used to control the coolant flow rate) reverts to fully open position. (c) An actuator freezes at where it was before the occurrence of the fault.

on FDI can be broadly categorized into model-based and data-based approaches. In the model-based approach, the information embodied in a process (identification or deterministic) model is utilized to detect and isolate faults (see [4–10] for reviews). In this approach, residuals are generated as fault indicators by using the analytical redundancy extracted from a process model. Faults are detected by checking whether or not the residuals breach their thresholds, and isolated using certain isolation logic. As shown in Fig. 1.3, the residual r_i is below its threshold $t_{h,i}$ under normal conditions. A fault is detected via the residual breaching its threshold after the occurrence of the fault at time t_f. This approach has been studied extensively for linear systems (see, e.g., [6, 8, 11–20]). The existing results include the parity space approach, the observer approach, the fault detection filter approach, and the parameter identification approach (see, e.g., [6]). The basic idea of the parity approach is to build parity equations that contain errors only due to the faults (see, e.g., [14]). This can be achieved by using only measurements (i.e., the direct redundancy) or the dynamic relationship between inputs and outputs (i.e, the temporal redundancy). In the observer approach, the basic idea is to reconstruct the system outputs from the measurements or subsets of the measurements by using Luenberger observers (see, e.g., [12, 13]) or Kalman filters (see, e.g., [11, 19]). This approach has been studied using dedicated observer schemes (see, e.g., [12, 13]) and generalized observer schemes (see, e.g., [6]), which differ in the relationship between faults and the sources of information used in building the residuals. Their ideas can be illustrated through sensor fault isolation. In the dedicated observer approach, each observer is driven by a different single sensor. A fault is isolated through a voting mechanism: the observer that gives state estimates significantly different from the majority indicates a fault in the corresponding sensor. In a generalized observer approach, each observer is driven by all the outputs except for a particular sensor. In this scheme, a fault is isolated when all the residuals breach their thresholds except for

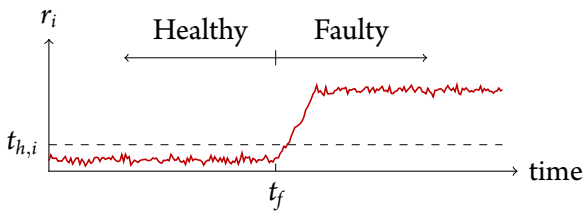

Figure 1.3: Illustration of the detection of a fault. Under normal conditions, the residual r_i is below its threshold $t_{h,i}$. A fault is detected via the residual breaching its threshold after the occurrence of the fault at time t_f.

the one that is generated without using measurements from the faulty sensor. Due to the presence of plant-model mismatch, residuals that are sensitive to faults but insensitive to modeling uncertainty are desired. To generate robust residuals, unknown input observers are developed to decouple the effect of unknown inputs, such as disturbances, from that of the faults on the evaluation of the residuals (see, e.g., [16]). In the fault detection filter approach (see, e.g., [6]), the objective is to design a full-order state observer with a special choice of the feedback gain matrix in the observer design. It is chosen such that the residuals have certain directional properties at the occurrence of certain fault. In addition to the above three approaches, faults can be identified through parameter identification (see, e.g., [6]). In this approach, the model parameters are estimated by using the system model and input/output data. The declaration of a fault is made using the relationship between faults and deviations between the nominal values of the physical parameters and their estimates.

Recently, the problem of FDI has also be studied for nonlinear systems (see, e.g., [21–31]), hybrid systems (see, e.g, [32]), and distributed parameter systems (see, e.g., [33–36]). In [22], a nonlinear FDI filter is designed to solve a fundamental problem of residual generation for nonlinear systems subject to actuator/process faults by using a geometric approach. The objective of the filter design is to build a dynamic system for the generation of residuals that are affected by a particular fault and decoupled from disturbances and the rest of faults. The isolation of actuator faults is also studied by exploiting the system structure to generate dedicated residuals [27]. In this approach, each residual, which is defined as the discrepancy between the state measurement and its expected trajectory, is uniquely sensitive to one fault. While uncertainty is not explicitly considered, the thresholds can be appropriately relaxed in the practical implementation of this approach. This approach has also been studied using asynchronous measurements [28] and applied in the context of distributed MPC [37], and the effectiveness demonstrated through application to a catalytic alkylation of benzene process [38]. To handle unstructured modeling uncertainty,

adaptive estimation techniques are used to generate residuals (i.e., the output estimation errors) through a bank of estimators and time-varying thresholds for a class of Lipschitz nonlinear systems subject to actuator/process faults [23, 29] and sensor faults [24, 31]. In this approach, a group of residuals are generated to detect faults first. Upon fault detection, a group of isolation residuals are generated for each fault. In the fault isolation logic, any residual breaching its threshold excludes a fault associated to the corresponding group of residuals. Therefore, a fault is isolated when all the other groups have residuals breaching their thresholds except for the one associated to that fault. For systems modeled by polynomial differential algebraic equations, analytical redundancy relations, which are constructed by eliminating the unknown state variables through a successive derivation of the system inputs and outputs, are used to generate structured residuals for FDI (see, e.g., [21]). In addition to nonlinear systems, the problem of fault detection is studied for hybrid systems [32], which operate among multiple modes with different system dynamics. In comparison to FDI of nonlinear systems, the active mode where a hybrid system operates is first identified using a family of dedicated mode observers. Once the active mode is determined, a corresponding fault detection scheme is activated, where a time-varying bound on the derivative of a Lyapunov function is used as a dedicated threshold to detect actuator faults. In summary, the model-based approach to FDI is able to provide an explicit and insightful relationship between faults and their symptoms, such as residuals breaching their thresholds, through the use of a process model.

The data-based approach to FDI uses the information contained in past plant operating data to detect and isolate faults through multivariate statistical process monitoring (see, e.g., [39–43] and [44] for a review). From normal plant operating data, empirical correlation models can be built by using multivariate latent variable methods (see, e.g., [45]), such as principal component analysis (PCA) and partial least squares (PLS), which have been successfully applied in process industries. These models are low dimensional and can capture the key information in normal process data. The current process data are compared with the normal variation contained in these low dimensional models, and abnormal behavior is detected through statistical tests via statistics such as Hotelling's T^2 and squared prediction error (SPE). Faults can then be isolated by analyzing the contributions to the principal components from the individual variables using contribution plots (see, e.g., [46, 47]), which are able to isolate simple faults (i.e., those that only affect a particular variable). The isolation of complex faults (i.e., those that affect other variables) is improved by using additional data on past faults (see, e.g., [48]). The major benefits of this approach are that it does not require first principles models, it can handle a large number of measured variables, and process disturbances and measurement noise can be handled in a statistical

way. The fault isolation design, however, strongly relies on the availability of data on past faults (which in essence, provide a data-driven model for faulty operation), which may not always be available for fault diagnosis. The extensions of this approach include multiway PCA and PLS analysis [49], multiblock PLS methods [46], dynamic PCA [50], etc. In the methods using PCA and PLS, the statistical confidence limits of T^2/SPE statistics rely on the assumption that the process data have a multivariate normal distribution. This assumption, however, may not hold in practice due to reasons such as process nonlinearity, production strategy changes, feedstock and operating condition shifts, etc. [51]. Motivated by this consideration, the recent advances in the data-based approach have addressed the problem of dealing with nonnormality in process operating data and system nonlinearity using independent component analysis (see, e.g, [52]), statistics pattern analysis [53, 54], and nonlinear kernel Gaussian mixture models [51]. In the independent component analysis, a small number of independent variables are identified as the essential variables driving the process. These variables are expressed as linear combinations of the measured variables and found through algorithms that maximize the high-order statistics. In the statistics pattern analysis, the process behavior is captured by statistics of the process variables, which are computed from the batch trajectory for batch processes and a window of process measurements for continuous processes. Some deviation from the distribution of the process statistics under normal operation would be observed if the process behavior becomes abnormal. In the nonlinear kernel Gaussian mixture model based approach, the process data is projected into a high-dimensional kernel feature space. A Gaussian mixture model is estimated in the feature space, each component of which satisfies multivariate Gaussianity. The inferential index across different kernel Gaussian components is derived for fault detection. This index is then decomposed into variable contributions for fault diagnosis. In addition to the aforementioned model and data-based approaches, other approaches to FDI include those that use artificial neural networks [55] and Bayesian belief networks [56, 57].

In addition to FDI, the problem of FTC has also been extensively studied (see, e.g., [25, 27, 33, 35, 58–65]). Most existing results are developed based on the assumption of the availability of sufficient residual control effort or redundant control configurations that is able to preserve operation at the nominal equilibrium point under faulty conditions. The results in this direction can be broadly categorized into passive and active FTC approaches. In the passive approach, the key idea is to design reliable control structures such that the controller is able to preserve nominal operation in the absence of certain control loops resulting from faults (see, e.g., [60–63]). For linear systems, there have been results using robust pole region assignment [61] and modified linear-quadratic (LQ) regulator [60].

In [61], the state feedback gain is appropriately designed so that all combinations of actuator faults will not lead to any closed-loop system eigenvalue moving outside a stability region. The reliable LQ regulator designed in [60] possesses the properties of a standard LQ regulator. Furthermore, it guarantees system stability and a known quadratic performance bound in the presence of a selected subset of actuators by appropriately choosing a state-weighing matrix in the regulator design. This approach has also been studied for systems having unknown nonlinear dynamics (e.g., as a result of linearization of a nonlinear plant) with a boundedness condition [62, 63]. In these results, the set of actuators are divided into two groups. Only one group of actuators are susceptible to faults. The reliability with respect to faults relies on the use of the other group of actuators. The passive approach typically dictates the use of as many control loops as possible (i.e., control equipment redundancy) at the same time so that the failure of one control loop does not lead to the failure of the entire control system. Economic considerations, however, often require the use of only as many control loops as necessary to minimize the cost of control action, which may invalidate the passive methods. For this case, the problem of FTC has been studied using an active approach, where an appropriate backup control configuration is used to preserve nominal operation through control reconfiguration. The control configurations differ in the sets of the control equipment used. This approach, aided by the development of control tools (see, e.g., [66–72]), has been used to handle actuator (see, e.g., [25, 27, 33, 35, 64, 65]) and sensor (see, e.g., [58, 65]) faults. For the handling of actuator faults, this approach requires information on the location of a fault and therefore requires the presence of an FDI system. The backup control configuration should not use the failed control equipment. Furthermore, it should be able to guarantee closed-loop stability for the system starting from where the fault is detected and isolated (or the backup control configuration is activated). This is achieved by choosing the one under which the system state at the time of FDI is within the stability region of the nominal operating point. An explicit characterization of a stability region for each control configuration can be provided by nonlinear control designs (see, e.g., [72, 73]). The approach, however, is constrained by the availability of backup control configurations.

In practice, there exist numerous situations where faults can significantly hamper the available control action and consequently preclude the continuation of nominal operation regardless of the control law used (e.g., there does not exist sufficient residual control effort or backup control configurations). If the controller still tried to maintain nominal operation in this case, it could result in suboptimal operation or even process instability. As illustrated by the dashed line in Fig. 1.4, this could result in certain process variables exceeding their limits, which may necessitate shutting down an individual unit or even the

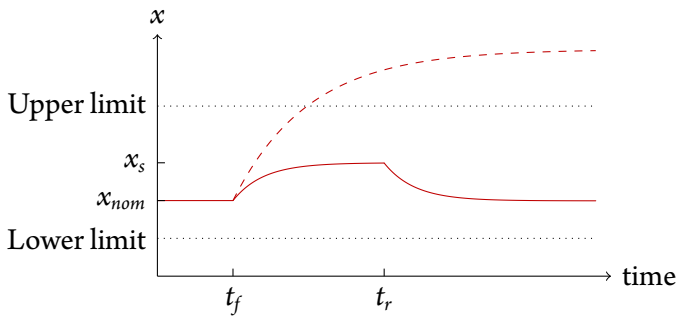

Figure 1.4: Illustration of safe-parking for FTC. The absence of safe-parking may result in process instability (dashed line) and lead to the state exceeding the limits (dotted lines). In contrast, operation at a safe-parking point x_s leads to safe and stable operation between the fault occurrence time t_f and the fault repair time t_r, and smooth resumption of operation at the nominal operating point x_{nom} after the fault is repaired (solid line).

entire plant, incurring significant economic losses. To address this problem, a safe-parking framework has recently been proposed to handle severe actuator faults (i.e., those that preclude the possibility of the continuation of nominal operation) in nonlinear process systems [74]. The key idea is to operate the plant at an appropriately chosen temporary equilibrium point (the so-called safe-park point) that enables safe and stable operation in the presence of the fault and smooth resumption of nominal operation after the fault is repaired (see the solid line in Fig. 1.4). The safe-parking framework provides a systematic way to design possible safe-park points off-line and to choose a safe-park point on-line (a safe-park point needs to satisfy certain conditions) depending on where the fault takes place and the state of the process at the time of FDI. Specifically, a safe-park point should be an equilibrium point subject to the fault and the process state should be within the stability region of a safe-park point at the time of FDI. This guarantees that the process can be stabilized and operate at a safe-park point under faulty conditions. In addition, the neighborhood of the safe-park point should be within the stability of the nominal operating point, which ensures that the process can be stabilized at the nominal operating point from the neighborhood of the safe-park point after the fault is repaired. The idea of safe-parking has been generalized to handle uncertainty and unavailability of full state measurements [75] and to handle faults for units interconnected in series [76] and transport-reaction processes [77]. The effectiveness of this approach has been demonstrated through application to a styrene polymerization process [78].

1.3 Objectives and Outline

A close examination of the literature indicates a lack of fault diagnosis methods that explicitly account for process nonlinearity exhibited by most chemical processes and the unavailability of full state measurements while providing insights to the causal relationship between faults and their symptoms. In addition, while there is a plethora of separate results on FDI and FTC, there is a lack of results on integrating FDI and FTC methods to deal with faults in a unified framework. To address these problems, the objectives of this thesis are as follows:

1. To explore how to utilize control action and process nonlinearity for isolation of complex actuator faults and process disturbances.
2. To develop a sensor fault isolation method that explicitly accounts for process nonlinearity and the unavailability of full state measurements.
3. To develop safe-parking techniques for handling severe actuator faults and addressing several issues for practical implementation.
4. To integrate FDI and FTC methods for detecting, isolating, and handling actuator or sensor faults seamlessly.
5. To illustrate the applications of the developed FDI and FTC methods to chemical process systems with nonlinear dynamics.

The rest of the thesis is organized as follows:

In Chapter 2, an active fault isolation method is proposed for nonlinear process systems subject to uncertainty. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory control. To this end, a dedicated fault isolation residual and its time-varying threshold are generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. These residuals, however, may not be sensitive to faults under nominal operation. To make these residuals sensitive to faults, a switching rule is designed to drive the process states, upon detection of a fault using any fault detection methods, to move towards an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea is then generalized to sequentially operate the process at multiple operating points that facilitate isolation of

different faults. The effectiveness of the proposed method is illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization of methyl methacrylate (MMA) and vinyl acetate (VAc).

In addition to actuator FDI, a sensor fault isolation and FTC design is proposed for nonlinear systems subject to input constraints in Chapter 3. The key idea of the proposed method is to exploit model-based sensor redundancy through state observer design. To this end, a high-gain observer is first presented and the stability property of the closed-loop system is rigorously established. By exploiting the enhanced applicability of the observer design, a fault isolation scheme is then proposed, which consists of a bank of observers, with each driven by a subset of the measured outputs. The residuals are defined as the discrepancies between the state estimates and their expected trajectories. A fault is isolated when all the residuals breach their thresholds except for the one that is generated without using measurements from the faulty sensor. After the fault is isolated, the state estimate generated using measurements from the healthy sensors is used in closed-loop to continue nominal operation. The implementation of the fault isolation and handling framework subject to uncertainty and measurement noise is illustrated using a chemical reactor example.

In Chapter 4, the problem of handling actuator faults is addressed for switched nonlinear process systems that transit between multiple modes subject to input constraints. The faults considered preclude the possibility of operation at the nominal equilibrium point in the active mode. Two cases are considered according to whether or not the switching schedule can be altered during the production process. For the case where the switching schedule is fixed, a safe-parking scheme is designed, which accounts for the switched nature, to operate the process at successive safe-park points as it transits to successive modes, which allow resumption of nominal operation after the fault is repaired. For the case where the switching schedule is adjustable, a safe-switching scheme is designed, which exploits the switched nature, to switch the process to a mode (if exists and available) where nominal operation can be preserved (through control structure reconfiguration when necessary) to continue nominal operation. The key ideas of the proposed framework are illustrated via a switched chemical reactor example, and the robustness with respect to uncertainty and measurement noise is demonstrated on an MMA polymerization process.

In Chapter 5, the safe-parking techniques developed for an isolated unit are generalized to account for the network structure of a chemical plant where multiple units are interconnected through an intricate network, with FDI and safe-parking techniques integrated in a unified framework. To this end, a robust FDI design is first presented, where relations between the prescribed inputs and state measurements in the absence of faults are con-

structed with the consideration of uncertainty. A fault is detected and isolated when the corresponding relation is violated. An algorithm is then developed to determine the units that need to be safe-parked during the fault repair period and generate possible safe-park points for the affected units. The implementation of the safe-parking techniques is triggered by the isolation of a fault, which can localize the effect of the fault in a subsystem of the networked plant. The efficacy of the integrated FDI and safe-parking framework is demonstrated on a chemical process example comprising three reactors and a separator.

The assumption of the *a priori* knowledge about the position of the failed actuator is relaxed to consider the case where a failed actuator is frozen at an arbitrary position in Chapter 6. This problem is studied by integrating fault diagnosis and safe-parking techniques. To this end, a model-based fault diagnosis design is proposed, which can not only identify the failed actuator, but also estimate the fault magnitude. The fault information is obtained by estimating the outputs of the actuators and comparing them with the corresponding prescribed control inputs. This methodology is first developed under state feedback control and then generalized to deal with state estimation errors. In the safe-parking design, possible safe-park points are generated for a series of design values of the failed actuator position. After a fault is diagnosed, the estimate of the failed actuator position is used to choose a safe-park point. The discrepancy between the actual value of the failed actuator position and the corresponding design value is handled through the robustness of the control design. The efficacy of the integrated fault diagnosis and safe-parking framework is demonstrated through a chemical reactor example.

Finally, Chapter 7 summarizes the main contributions of this thesis and suggests research opportunities for future work.

Chapter 2

Active Fault Isolation of Nonlinear Process Systems[1]

2.1 Introduction

In literature, the problem of FDI has been extensively studied by assuming the ability to isolate faults under the controller designed for nominal operation (i.e., the nominal controller). This approach is passive in the sense that the input/output data used for FDI are collected under the controller designed *only* for the purpose of stabilizing the process at the nominal operating point. For nonlinear process systems, the problem has been studied using dedicated residuals, which are generated by exploiting the structure of the system (see, e.g., [27]). In the required structure, for each fault, there exists a process state variable that is directly and uniquely affected by that fault. This implies that the fault variable is the only one that appears on the right-hand side of the differential equation for the corresponding state variable. The passive approach, however, may not remain effective if the structure of the closed-loop system inherently does not allow isolation of certain faults under the nominal controller. For example, the method in [27] does not remain valid for the case where multiple faults affect the evolution of the same state variable.

[1] The results in this chapter have been published in or submitted to:

a. M. Du and P. Mhaskar. Active fault isolation of nonlinear systems. In *Proceedings of the 2012 American Control Conference*, pages 6667–6672, Montréal, Canada, 2012.

b. M. Du and P. Mhaskar. Active fault isolation of nonlinear process systems. *AIChE J.*, provisionally accepted on August 31, 2012.

In comparison, there exist limited results on utilizing control action (e.g, feedback or supervisory control) to facilitate fault isolation, which has been paid attention until recently. We refer to this approach as active fault isolation. Along this line, a feedback control law has recently been utilized to enforce a closed-loop system structure by decoupling the dependency between certain state variables, which enhances the isolation of faults through data-based methods, under the assumption of full state measurements [81]. More recently, this approach has been extended to handle the case where only output measurements are available and studied with the use of MPC to optimize the input cost [82]. These results, however, do not address the problem of distinguishing between multiple faults that affect the evolution of the same process states. This problem is partly addressed for actuator faults by estimating the outputs of the actuators and comparing them with the corresponding prescribed values [83], where it is assumed that the outputs of the (healthy or failed) actuators are constant between two consecutive discrete times and there exists a subsystem of the plant that satisfies a full rank condition. In summary, while there are a plethora of results that rely on the ability to achieve FDI under nominal operation, the area of FTC stands to benefit from an active fault isolation framework that takes process nonlinearity and uncertainty into account, and more importantly enables FDI that might not otherwise be possible under nominal operation.

Motivated by the above considerations, this chapter considers the problem of designing an active fault isolation scheme for nonlinear process systems subject to uncertainty. The faults under consideration include bounded actuator faults and process disturbances that directly affect the evolution of the same process states. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory control. To this end, a dedicated fault isolation residual and its time-varying threshold are generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. These residuals, however, may not be sensitive to faults under nominal operation. To make these residuals sensitive to faults, a switching rule is designed to drive the process states, upon detection of a fault using any fault detection methods, to move towards an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea is then generalized to sequentially operate the process at multiple operating points that facilitate isolation of different faults. The effectiveness of the proposed method is illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization process

The rest of this chapter is organized as follows. The process description and a fault detection design are first presented in Section 2.2. A motivating example of a solution copoly-

merization of MMA and VAc is given in Section 2.3. An active fault isolation design is proposed in Section 2.4. The simulation results are presented in Section 2.5. Finally, Section 2.6 concludes with a summary of results.

2.2 Preliminaries

2.2.1 Process Description

Consider a nonlinear process system described by

$$\dot{x} = f(x) + G(x)u + w(x,t) + D(x)\theta(t) \tag{2.1}$$

where $x = [x_1, \ldots, x_n]^{\mathrm{T}} \in \mathbb{R}^n$ denotes the vector of state variables, $u \in \mathbb{R}^m$ denotes the vector of input variables, the vector and matrix functions $f = [f_1, \ldots, f_n]^{\mathrm{T}} : \mathbb{R}^n \to \mathbb{R}^n$ and $G = [g_1^{\mathrm{T}}, \ldots, g_n^{\mathrm{T}}]^{\mathrm{T}} : \mathbb{R}^n \to \mathbb{R}^n \times \mathbb{R}^m$ are smooth, the vector function $w = [w_1, \ldots, w_n]^{\mathrm{T}} : \mathbb{R}^n \times [0, \infty) \to \mathbb{R}^n$ denotes process uncertainty, $D(\cdot) = [d_1^{\mathrm{T}}(\cdot), \ldots, d_n^{\mathrm{T}}(\cdot)]^{\mathrm{T}}$ denotes a fault distribution matrix function, with $d_i = [d_{i1}(\cdot), \ldots, d_{iq}(\cdot)]$ and $d_{ij} : \mathbb{R}^n \to \mathbb{R}$ being a continuous function for $j = 1, \ldots, q$, and $\theta = [\theta_1, \ldots, \theta_q]^{\mathrm{T}} \in \mathbb{R}^q$ denotes the vector of faults, with $q \leq n$, which include actuator faults and process disturbances. To be able to differentiate between nominal uncertainty and faults, it is required that the system of Eq. (2.1) satisfy Assumption 2.1 below.

Assumption 2.1. For the system of Eq. (2.1), there exist known vector functions $w_l = [w_{1,l}, \ldots, w_{n,l}]^{\mathrm{T}} : \mathbb{R}^n \to \mathbb{R}^{-n}$ and $w_u = [w_{1,u}, \ldots, w_{n,u}]^{\mathrm{T}} : \mathbb{R}^n \to \mathbb{R}^{+n}$ such that

$$w_l(x) \leq w(x,t) \leq w_u(x) \tag{2.2}$$

for any $t \in [0, \infty)$.

Assumption 2.1 establishes bounding functions on uncertainty, which will be used in the robust fault detection design presented next.

2.2.2 Fault Detection Design

The fault isolation framework presented in this chapter requires a "trigger" resulting from fault detection. To this end, any of the existing fault detection methods can be utilized.

A representative one is presented and formalized in Theorem 2.1 below. The key idea is to estimate the bounds on the current values of the process states and determine whether or not the current state measurements are in between these bounds. These bounds are estimated using state measurements over a moving estimation horizon, which is defined as follows:

$$T = \begin{cases} t, & 0 \leq t < T' \\ T', & t \geq T' \end{cases} \tag{2.3}$$

where $T' > 0$ denotes the length of the horizon after the initialization period (i.e., after time T').

Theorem 2.1. *Consider the system of Eq. (2.1), for which Assumption 2.1 holds. Then, there exist vector functions* $x_l(t) = [x_{1,l}(t), \ldots, x_{n,l}(t)]^{\mathrm{T}}$ *and* $x_u(t) = [x_{1,u}(t), \ldots, x_{n,u}(t)]^{\mathrm{T}}$ *such that if* $x_i(t) \notin [x_{i,l}(t), x_{i,u}(t)]$ *for some* $i \in \{1, \ldots, n\}$, *then* $\theta(\tau) \neq 0$ *for some* $\tau \in [t-T, t]$. *Furthermore, if* $d_i(x)\theta(\tau) < w_{i,l}(x) - w_i(x,\tau)$ *for all* $\tau \in [t-T, t]$, *then* $x_i(t) < x_{i,l}(t)$. *Similarly, if* $d_i(x)\theta(\tau) > w_{i,u}(x) - w_i(x,\tau)$ *for all* $\tau \in [t-T, t]$, *then* $x_i(t) > x_{i,u}(t)$.

Proof. The proof is divided into two parts. In the first part, we show the existence of vector functions $x_l(t)$ and $x_u(t)$ such that if $x_i(t) \notin [x_{i,l}(t), x_{i,u}(t)]$ for some $i \in \{1, \ldots, n\}$, then $\theta(\tau) \neq 0$ for some $\tau \in [t-T, t]$. In the second part, we show that if $d_i(x)\theta(\tau) < w_{i,l}(x) - w_i(x,\tau)$ for all $\tau \in [t-T, t]$, then $x_i(t) < x_{i,l}(t)$. By following a similar line of arguments, it then can be shown that if $d_i(x)\theta(\tau) > w_{i,u}(x) - w_i(x,\tau)$ for all $\tau \in [t-T, t]$, then $x_i(t) > x_{i,u}(t)$.

Part 1: Consider the time interval $[t-T, t]$, with t being the current time. Integrating the system of Eq. (2.1) over $[t-T, t]$ yields

$$x(t) - x(t-T) = \tilde{f}(t) + \tilde{w}(t) + \int_{t-T}^{t} D(x)\theta(\tau)d\tau \tag{2.4}$$

where $\tilde{f}(t) = \int_{t-T}^{t}[f(x) + G(x)u]d\tau$ and $\tilde{w}(t) = [\tilde{w}_1(t), \ldots, \tilde{w}_n(t)]^{\mathrm{T}} = \int_{t-T}^{t} w(x,\tau)d\tau$. Let

$$x_l(t) = x(t-T) + \tilde{f}(t) + \tilde{w}_l(t) \tag{2.5}$$

and

$$x_u(t) = x(t-T) + \tilde{f}(t) + \tilde{w}_u(t) \tag{2.6}$$

where $\tilde{w}_l(t) = [\tilde{w}_{1,l}(t), \ldots, \tilde{w}_{n,l}(t)]^{\mathrm{T}} = \int_{t-T}^{t} w_l(x)d\tau$ and $\tilde{w}_u(t) = [\tilde{w}_{1,u}(t), \ldots, \tilde{w}_{n,u}(t)]^{\mathrm{T}} = \int_{t-T}^{t} w_u(x)d\tau$. Since $w_l(x) \leq w(x,\tau) \leq w_u(x)$ for any $\tau \in [t-T, t]$, it follows that if

$\theta(\tau) = 0$ for any $\tau \in [t-T, t]$, then the following equation holds

$$x_l(t) \leq x(t) \leq x_u(t) \tag{2.7}$$

Therefore, $x_i(t) \notin [x_{i,l}(t), x_{i,u}(t)]$ for some $i \in \{1, \ldots, n\}$ implies that $\theta(\tau) \neq 0$ for some $\tau \in [t-T, t]$.

Part 2: Since $d_i(x)\theta(\tau) < w_{i,l}(x) - w_i(x,\tau)$ for all $\tau \in [t-T, t]$, we have

$$\int_{t-T}^{t} d_i(x)\theta(\tau)d\tau < \int_{t-T}^{t} [w_{i,l}(x) - w_i(x,\tau)]d\tau = \tilde{w}_{i,l}(t) - \tilde{w}_i(t) \tag{2.8}$$

It follows from Eqs. (2.4), (2.5), and (2.8) that

$$x_i(t) - x_{i,l}(t) = \tilde{w}_i(t) - \tilde{w}_{i,l}(t) + \int_{t-T}^{t} d_i(x)\theta(\tau)d\tau < 0 \tag{2.9}$$

which implies that

$$x_i(t) < x_{i,l}(t) \tag{2.10}$$

This completes the proof of Theorem 2.1. □

Remark 2.1. The fault detection design of Theorem 2.1 explicitly accounts for process uncertainty. To this end, the lower and upper bounds, denoted by $x_l(t)$ and $x_u(t)$, on the process states at the current time t are evaluated by using the process model and measurements over an estimation horizon of length T subject to the possible realization of uncertainty. If no faults take place, the process states should comply with these bounds (i.e., $x(t) \in [x_l(t), x_u(t)]$). Because the computation of these bounds considers the worst effect of uncertainty, the only way that any state breaches its bounds is that a fault takes place. Consequently, the fault detection design is robust in the sense that there will be no false alarms before a fault takes place (albeit at the cost of "small faults" that are indistinguishable from the effect of uncertainty). In addition, the fault detection design of Theorem 2.1 can be used to group faults that possibly take place. Specifically, the fault that takes place is among the group of the ones for which the elements in the corresponding row of the fault distribution matrix function are non-zero. As a special case, if that group contains only one fault, then the fault is also isolated.

Remark 2.2. In addition to the fault detection mechanism, Theorem 2.1 also gives explicit conditions on the class of faults that are detectable. These conditions can be interpreted from two perspectives. First, the faults should make $d_i(x)\theta(\tau)$ remain negative or positive over the time interval $[t-T, t]$. Second, the magnitude of $d_i(x)\theta(\tau)$ should be large enough

over the same period (i.e., larger than that of the difference between $w_i(x,\tau)$ and $w_{i,l}(x)$ or $w_{i,u}(x)$). Although the satisfaction of these conditions guarantees that faults can be detected, the fault detection design is not limited to this particular class of faults. In fact, the integral form of these conditions exactly characterizes the class of faults that are detectable (e.g., $\int_{t-T}^{t} d_i(x)\theta(\tau)d\tau < \tilde{w}_{i,l}(t) - \tilde{w}_i(t)$ is used instead of $d_i(x)\theta(\tau) < w_{i,l}(x) - w_i(x,\tau)$ for all $\tau \in [t-T, t]$). It essentially considers possible changes in the sign of $d_i(x)\theta(\tau)$ and reflects the accumulating effect of faults. Note that faults that do not satisfy the conditions in the integral form may have similar effects as process uncertainty (reflecting the inherent tradeoff between robustness and fault sensitivity). If the process operates under an appropriately designed robust control law, they would not lead to instability of the closed-loop system.

2.3 Motivating Example: A Solution Copolymerization Reactor

In this section, we consider a solution copolymerization of MMA and VAc, where monomers A (MMA) and B (VAc) are continuously fed to a continuous-stirred tank reactor (CSTR) with initiator (azobisisobutyronitrile, AIBN), solvent (benzene), and chain transfer agent (acetaldehyde). A cooling jacket is equipped to remove the heat of the copolymerization reaction. The mathematical model for this reactor (in the absence of recycle streams and inhibitors) is of the following form [84]:

$$\begin{aligned}
\dot{C}_j &= \left(\frac{Q_j}{M_j} - \frac{C_j \sum_k Q_k}{\rho}\right)\frac{1}{V} - R_j, \quad j = a, b, i, s, t \\
\dot{T}_R &= (T_0 - T_R)\frac{\sum_k Q_k}{\rho V} + [(-\Delta H_{paa})k_{paa}C_a C_{a\cdot} + (-\Delta H_{pba})k_{pba}C_a C_{b\cdot} \\
&\quad (-\Delta H_{pab})k_{pab}C_b C_{a\cdot} + (-\Delta H_{pbb})k_{pbb}C_b C_{b\cdot}]\frac{1}{\rho c_p} - \frac{UA(T_R - T_c)}{\rho c_p V}
\end{aligned} \tag{2.11}$$

where C_j is the concentration of species j, with subscript a, b, i, s, and t denoting monomer A, monomer B, initiator, solvent, and chain transfer agent, respectively, T_R is the temperature in the reactor, Q_k is the mass flow rate of species k, $k = a, b, i, s, t$, T_c is the temperature in the cooling jacket, M_j is the molar mass of species j, V is the volume of the reactor, ΔH is the enthalpy of the reaction, ρ and c_p are the density and the heat capacity of the fluid in the reactor, respectively, U is the overall heat transfer coefficient, A is the heat transfer area

of the reactor, T_c is the temperature in the cooling jacket, and

$$
\begin{aligned}
R_a &= [(k_{paa} + k_{xaa})C_{a\cdot} + (k_{pba} + k_{xba})C_{b\cdot}]C_a \\
R_b &= [(k_{pbb} + k_{xbb})C_{b\cdot} + (k_{pab} + k_{xab})C_{a\cdot}]C_b \\
R_i &= k_i C_i \\
R_s &= (k_{xas}C_{a\cdot} + k_{xbs}C_{b\cdot})C_s \\
R_t &= (k_{xat}C_{a\cdot} + k_{xbt}C_{b\cdot})C_t \\
C_{a\cdot} &= \frac{-l_2 + \sqrt{l_2^2 - 4l_1l_3}}{2l_1} \\
C_{b\cdot} &= \beta C_{a\cdot} \\
l_1 &= k_{caa} + k_{daa} + 2\beta(k_{cab} + k_{dab}) + \beta^2(k_{cbb} + k_{dbb}) \\
l_2 &= 0 \\
l_3 &= -2k_i C_i \varepsilon \\
\beta &= \frac{(k_{pab} + k_{xab})C_b}{(k_{pba} + k_{xba})C_a}
\end{aligned}
$$

Each of the rate constants is computed through the Arrhenius equation

$$k = Ae^{-E/RT_R} \tag{2.13}$$

where A is the preexponential constant, E is the activation energy, and R is the ideal gas constant. The process parameters can be found in Table 2.1 (see also [84]).

The control objective under fault-free conditions is to operate the process at the nominal operating point, where $C_a = 2.534 \times 10^{-1}$ kmol/m^3, $C_b = 5.838$ kmol/m^3, $C_i = 2.008 \times 10^{-3}$ kmol/m^3, $C_s = 2.758$ kmol/m^3, $C_t = 3.663 \times 10^{-1}$ kmol/m^3, and $T_R = 350.5$ K. It is assumed that all the state measurements are available, and the flow rates Q_k, $k = a, b, i, s, t$, and the temperature in the cooling jacket T_c are chosen as manipulated input variables. The inputs are bounded as $0 \leq Q_a \leq 50$ kg/hr, $0 \leq Q_b \leq 120$ kg/hr, $0 \leq Q_i \leq 0.5$ kg/hr, $0 \leq Q_s \leq 100$ kg/hr, $0 \leq Q_t \leq 10$ kg/hr, and $320 \leq T_c \leq 350$ K. The steady state values of the inputs corresponding to the nominal operating point are $Q_a = 18$ kg/h, $Q_b = 90$ kg/h, $Q_i = 0.18$ kg/h, $Q_s = 36$ kg/h, $Q_t = 2.7$ kg/h, and $T_j = 336.15$ K. Linear model predictive control is implemented for the control purpose. The hold-time for the control action is chosen as $\Delta = 3$ min, control horizon $T_c = 2\Delta$, and the prediction horizon $T_p = 10\Delta$. In the objective function for model predictive control, the states are normalized against ranges $[0, 1]$, $[0, 8]$, $[0, 5\times10^{-3}]$, $[0, 10]$, $[0, 1]$,

Table 2.1: Process parameters for the solution copolymerization example of Section 2.3.

Parameter	Value	Unit	Parameter	Value	Unit
V	1	m^3	A_{xba}	5.257×10^4	m^3/kmol·s
R	8.314	kJ/kmol·K	A_{xbb}	1577	m^3/kmol·s
ρ	8.79×10^2	kg/m^3	A_{xbs}	1514	m^3/kmol·s
c_p	2.01	kJ/kg·K	A_{xbt}	4.163×10^5	m^3/kmol·s
U	6.0×10^{-2}	kJ/m^2·s·K	E_i	1.25×10^5	kJ/kmol
A	4.6	m^2	E_{caa}	2.69×10^4	kJ/kmol
T_0	353.15	K	E_{cbb}	4.00×10^3	kJ/kmol
ε	1		E_{daa}	0.0	kJ/kmol
M_a	100.12	kg/kmol	E_{dbb}	0.0	kJ/kmol
M_b	86.09	kg/kmol	E_{paa}	2.42×10^4	kJ/kmol
M_i	164.21	kg/kmol	E_{pab}	2.42×10^4	kJ/kmol
M_s	78.11	kg/kmol	E_{pba}	1.80×10^4	kJ/kmol
M_t	44.05	kg/kmol	E_{pbb}	2.42×10^4	kJ/kmol
A_i	4.5×10^{14}	s^{-1}	E_{xaa}	2.42×10^4	kJ/kmol
A_{caa}	4.209×10^{11}	m^3/kmol·s	E_{xab}	2.42×10^4	kJ/kmol
A_{cbb}	1.61×10^9	m^3/kmol·s	E_{xas}	2.42×10^4	kJ/kmol
A_{daa}	0	m^3/kmol·s	E_{xat}	2.42×10^4	kJ/kmol
A_{dbb}	0	m^3/kmol·s	E_{xba}	1.80×10^4	kJ/kmol
A_{paa}	3.207×10^6	m^3/kmol·s	E_{xbb}	1.80×10^4	kJ/kmol
A_{pab}	1.233×10^5	m^3/kmol·s	E_{xbs}	1.80×10^4	kJ/kmol
A_{pba}	2.103×10^8	m^3/kmol·s	E_{xbt}	2.42×10^4	kJ/kmol
A_{pbb}	6.308×10^6	m^3/kmol·s	$-\Delta H_{paa}$	54.0×10^3	kJ/kmol
A_{xaa}	32.08	m^3/kmol·s	$-\Delta H_{pba}$	54.0×10^3	kJ/kmol
A_{xab}	1.234	m^3/kmol·s	$-\Delta H_{pab}$	86.0×10^3	kJ/kmol
A_{xas}	86.6	m^3/kmol·s	$-\Delta H_{pbb}$	86.0×10^3	kJ/kmol
A_{xat}	2085.0	m^3/kmol·s			

and $[340, 355]$, respectively, and the inputs are done against the constraints. The matrices used to penalize the deviations of the normalized states from the steady state values and the increments of the inputs are diag$[1, 1, 1, 1, 1, 1]$ and diag$[1, 1, 50, 0.5, 1, 1]$, respectively.

Practical issues, such as parametric uncertainty, time-varying disturbances, and measurement noise, are considered in the simulations. Specifically, the values of A_{pab}, A_{pba}, A_{paa}, A_{pbb}, A_{xas}, A_{xbs}, A_{xat}, and A_{xbt} are 10% smaller than their nominal values, and those of A_{xab}, A_{xba}, A_{xaa}, and A_{xbb} are 10% larger. The bounds on these uncertainty are $\pm 15\%$ of their nominal values. It is assumed that the inlet streams of monomer B and solvent are impure. There exist a small amount of solvent and monomer B in the flows of monomer B and solvent, respectively. The mass fraction of monomer B in the flow of solvent is described by $0.02 + 0.02 \sin(t)$, and the mass fraction of solvent in the flow of monomer B is

$0.01 + 0.01\sin(2t)$. The upper bounds on the magnitudes of disturbances in the streams of monomer B and solvent are 3% and 5%, respectively. The measurement noise has a normal distribution of variance 0.02, 0.2, 0.0005, 0.2, 0.02, and 0.5 in C_a, C_b, C_i, C_s, C_t, and T_R, respectively. It is assumed that measurements are sampled 20 times evenly between two successive times when control action is implemented. The noisy measurements are preprocessed through a moving average filter, which takes the mean of the previous 20 samples, before used for control and FDI.

Consider actuator faults in the process of Eq. (2.11), which are denoted by θ_j, $j = 1$, ..., 6, for faults in Q_a, Q_b, Q_i, Q_s, Q_t, and T_c, respectively. The faults are assumed to be bounded as $|\theta_1| \leq 4.5$ kg/hr, $|\theta_2| \leq 25$ kg/hr, $|\theta_3| \leq 9$ kg/hr, $|\theta_4| \leq 25$ kg/hr, $|\theta_5| \leq 0.675$ kg/hr, and $|\theta_6| \leq 5$ K. The expression of the fault distribution matrix is as follows:

$$D = \frac{1}{V}\begin{bmatrix} \frac{1}{M_a} - \frac{C_a}{\rho} & -\frac{C_a}{\rho} & -\frac{C_a}{\rho} & -\frac{C_a}{\rho} & -\frac{C_a}{\rho} & 0 \\ -\frac{C_b}{\rho} & \frac{1}{M_b} - \frac{C_b}{\rho} & -\frac{C_b}{\rho} & -\frac{C_b}{\rho} & -\frac{C_b}{\rho} & 0 \\ -\frac{C_i}{\rho} & -\frac{C_i}{\rho} & \frac{1}{M_i} - \frac{C_i}{\rho} & -\frac{C_i}{\rho} & -\frac{C_i}{\rho} & 0 \\ -\frac{C_s}{\rho} & -\frac{C_s}{\rho} & -\frac{C_s}{\rho} & \frac{1}{M_s} - \frac{C_s}{\rho} & -\frac{C_s}{\rho} & 0 \\ -\frac{C_t}{\rho} & -\frac{C_t}{\rho} & -\frac{C_t}{\rho} & -\frac{C_t}{\rho} & \frac{1}{M_t} - \frac{C_t}{\rho} & 0 \\ \frac{T_0 - T_R}{\rho} & \frac{T_0 - T_R}{\rho} & \frac{T_0 - T_R}{\rho} & \frac{T_0 - T_R}{\rho} & \frac{T_0 - T_R}{\rho} & \frac{UA}{\rho c_p} \end{bmatrix} \tag{2.14}$$

The above expression shows a typical case where there exist multiple faults that may directly affect the evolution of the same process states. For example, all the faults in the flow rate actuators directly affect the evolution of the concentration of monomer A, as well as all the other state variables. For this case, the system is not of the structure that can be utilized to build dedicated residuals as in [27]. The FDI design in [81] would at best identify a group of possible faults, which may include all the faults in the worst case. Therefore, the process complexity asks for FDI designs that take into account the nonlinear way (in the sense that the fault distribution matrix is not constant, but a function of the process states) that faults affect the process evolution, as well as nonlinear dynamics and process uncertainty, motivating the fault-isolation approach presented next.

2.4 Active Fault Isolation Design

In this section, we present an active fault isolation scheme. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory feedback control. To this end, a special operating point termed fault isolation

point is first defined, the property of which can be used to differentiate between multiple faults. In general, the fault isolation point is not identical to the nominal operating point. For the purpose of fault isolation, a switching rule is then designed to drive the process states to move towards a fault isolation point upon detection of a fault using any fault detection methods. To distinguish a particular fault from other faults, we require information on the magnitudes of faults, which are characterized in Assumption 2.2 below.

Assumption 2.2. For the system of Eq. (2.1), $\theta_l \leq \theta \leq \theta_u$, where $\theta_l = [\theta_{1,l}, \ldots, \theta_{q,l}]^{\mathrm{T}} \in \mathbb{R}^{-q}$ and $\theta_u = [\theta_{1,u}, \ldots, \theta_{q,u}]^{\mathrm{T}} \in \mathbb{R}^{+q}$ denote the lower and upper bounds on θ, respectively.

Remark 2.3. The focus of this chapter is to design a methodology that is able to isolate complex faults for the case where multiple faults simultaneously appear on the right hand side of a differential equation for the same state variable. Note that if the faults considered are unbounded, then any fault that takes place may be seen as the occurrence of any one of the other faults that affect the evolution of the same state no matter how small the values of the corresponding weighting coefficient functions (i.e., $d_{ij}(\cdot)$ in the fault distribution matrix function) are. In contrast, this chapter considers faults such as biases or drifts, which are commonly encountered in practice, and take place due to control actuator malfunctions or process abnormalities, such as leakage of feedstocks. These faults can be modeled as bounded (although possibly time-varying) variables as formalized in Assumption 2.2.

We next define a fault isolation point, which will be used to generate appropriate control action through a switching rule for fault isolation.

Definition 2.1. A point $\tilde{x}$ is a fault isolation point if there exists $\tilde{u} \in \mathbb{R}^m$ such that $f(\tilde{x}) + G(\tilde{x})\tilde{u} = 0$, and for any fault θ_j, $j = 1, \ldots, q$, there exists a state x_i, $i \in \{1, \ldots, n\}$ such that $d_{ik}(\tilde{x}) = 0$ for all $k \in \{1, \ldots, q\} \backslash \{j\}$ and $d_{ij} \neq 0$ for any $x \in D$, where $D \subseteq \mathbb{R}^n$.

Remark 2.4. Note that a fault isolation point needs to satisfy three conditions. First, it is an equilibrium point for the nominal system (i.e., the system of Eq. (2.1) with $w(x,t) \equiv 0$ and $\theta(t) \equiv 0$). This requirement makes it possible to operate at a fault isolation point, at which the remaining two conditions are defined. Second, for a given fault, at a fault isolation point, there exists at least one system state for which that fault is the only one that essentially appears on the right hand side of the corresponding differential equation. This requirement makes it possible to isolate a given fault (even if the third condition is not satisfied; see Remark 2.9 for a further discussion). Finally, it is also required that the second condition is satisfied for all the faults under consideration. This requirement implies that the number of state variables should not be less than that of the faults, and makes it possible to isolate multiple faults.

Remark 2.5. Note that if the fault distribution matrix function is constant (e.g., in the case of a linear system, but not necessarily), there may not exist a fault isolation point for the original system. However, the system could be transformed through a coordinate transformation into the one to which existing methods (e.g., [27]) can be applied. To illustrate this point, we decompose the system state of Eq. (2.1) as follows: $x = [x_d^{\mathrm{T}}, x_{\bar{d}}^{\mathrm{T}}]^{\mathrm{T}}$, where $x_d \in \mathbb{R}^q$ and $x_{\bar{d}} \in \mathbb{R}^{n-q}$, and consider the x_d subsystem described by $\dot{x}_d = f_d(x) + G_d(x)u + w_d(x,t), +D_d\theta(t)$, where D_d is constant, and $f_d(\cdot)$, $G_d(\cdot)$, and $w_d(\cdot,\cdot)$ are appropriately defined. Multiplying both sides of the x_d subsystem by D_d^{-1} (if D_d is invertible) and defining a state vector $\hat{x}_d = D_d^{-1}x_d$ yields an equivalent subsystem described by $\dot{\hat{x}}_d = f_d(\hat{x}) + G_d(\hat{x}) + w_d(\hat{x},t) + \theta(t)$, where $\hat{x} = [(D_d\hat{x}_d)^{\mathrm{T}}, x_{\bar{d}}^{\mathrm{T}}]^{\mathrm{T}}$. The system in the transformed coordinate satisfies the structure requirement specified in [27], where it is assumed that for each fault, there exists a state variable whose evolution is directly and uniquely affected by that fault. Therefore, this case can be handled by existing methods, and would not necessitate an active fault isolation scheme.

A distinguishing feature of the proposed method is that control action is utilized for the purpose of fault isolation. In particular, we propose to move the process to a fault isolation point upon fault detection, close to which the property of the fault distribution matrix can be utilized to differentiate between complex faults. This naturally implies that in the presence of faults, there should remain sufficient control effort that enables moving the process to a fault isolation point. Note that the proposed method satisfies a very specific fault isolation need. In particular, it addresses the kind of faults which does not pose an immediate threat to the stability or operation of the process. In other words, under the occurrence of faults, nominal operation could still be continued (and, under the proposed method, the remaining control effort allows moving the process in the presence of faults). The motivation for fault isolation in this case is to catch a fault before it possibly turns into a bigger catastrophic failure. Note also that the work in this chapter does not require a specific control design. Any robust control law that satisfies the property stated in Assumption 2.3 below can be used to move the process states.

Assumption 2.3. For the system of Eq. (2.1), there exists a robust control law $RC(x)$ such that given any $x(0) \in D$ and $d > 0$, there exists a finite positive real number T_c such that $x(t) \in B_d$ for all $t \geq T_c$, where $D \subseteq \mathbb{R}^n$ and B_d is closed ball of radius d around $\tilde{x}$.

Assumption 2.3 establishes the ability to drive the process states to an arbitrarily small neighborhood of a fault isolation point $\tilde{x}$ for any initial condition within some region D in finite time even under faulty conditions. With this ability available, the active fault isolation

design is formulated in Theorem 2.2 below. To this end, let t_d denote the time that a fault is detected, and u_x and $u_{\tilde{x}}$ denote the control inputs to stabilize the system of Eq. (2.1) at the nominal equilibrium point and a fault isolation point, respectively.

Theorem 2.2. *Consider the system of Eq. (2.1), for which $\tilde{x}$ is a fault isolation point and Assumptions 2.1-2.3 hold. Then, given a fault θ_j for any $j \in \{1, \ldots, q\}$, there exist functions $\tilde{x}_{i,l}(t)$ and $\tilde{x}_{i,u}(t)$ such that if $x_i(t) \notin [\tilde{x}_{i,l}(t), \tilde{x}_{i,u}(t)]$, then $\theta_j(\tau) \neq 0$ for some $\tau \in [t-T, t]$. Furthermore, there exists $d > 0$ and $T_c' > 0$ such that under the switching rule*

$$u(t) = \begin{cases} u_x(t), & 0 \leq t < t_d \\ u_{\tilde{x}}(t), & t \geq t_d \end{cases} \tag{2.15}$$

if $x(t_d) \in D$, then for $t \geq T_c'$, $x_i(t) \notin [x_{i,l}(t), x_{i,u}(t)]$ implies $x_i(t) \notin [\tilde{x}_{i,l}(t), \tilde{x}_{i,u}(t)]$.

Proof. The proof is divided into two parts. In the first part, we show that there exist threshold functions $\tilde{x}_l(t)$ and $\tilde{x}_u(t)$ such that if the corresponding state measurement breaches these thresholds, then a fault is isolated. In the second part, we show that under the switching rule of Eq. (2.15), for a given fault, if it can be differentiated from plant-model mismatch, then it can also be isolated as long as the system state is close enough to the fault isolation point.

Part 1: Consider the following equation

$$\begin{aligned} \dot{x}_i &= f_i(x) + g_i(x)u + w_i(x,t) + d_i(x)\theta(t) \\ &= f_i(x) + g_i(x)u + w_i(x,t) + h_i(x,t) + d_{ij}(x)\theta_j(t) \end{aligned} \tag{2.16}$$

where $h_i(x,t) = \sum_{k=1,k\neq j}^{q} d_{ik}(x)\theta_k(t)$. Integrating the above equation over $[t-T, t]$ yields

$$x_i(t) - x_i(t-T) = \tilde{f}_i(t) + \tilde{w}_i(t) + \tilde{h}_i(t) + \int_{t-T}^{t} d_{ij}(x)\theta_j(\tau)d\tau \tag{2.17}$$

where $\tilde{f}_i(t) = \int_{t-T}^{t}[f_i(x) + g_i(x)u]d\tau$ and $\tilde{h}_i(t) = \int_{t-T}^{t}\sum_{k=1,k\neq j}^{q} d_{ik}(x)\theta_k(\tau)d\tau$. The lower and upper bounds on $\tilde{h}_i(t)$ are estimated as follows:

$$\tilde{h}_{i,l}(t) = \int_{t-T}^{t} \sum_{k=1,k\neq j}^{q} d_{ik}(x)\hat{\theta}_{k,l}(\tau)d\tau \tag{2.18}$$

and

$$\tilde{h}_{i,u}(t) = \int_{t-T}^{t} \sum_{k=1,k\neq j}^{q} d_{ik}(x)\hat{\theta}_{k,u}(\tau)d\tau \tag{2.19}$$

where $\hat{\theta}_{k,l} = \begin{cases} \theta_{k,u}, & \text{if } d_{ik}(x) \leq 0 \\ \theta_{k,l}, & \text{if } d_{ik}(x) > 0 \end{cases}$ and $\hat{\theta}_{k,u} = \begin{cases} \theta_{k,l}, & \text{if } d_{ik}(x) \leq 0 \\ \theta_{k,u}, & \text{if } d_{ik}(x) > 0 \end{cases}$. Let

$$\tilde{x}_{i,l}(t) = x_i(t-T) + \tilde{f}_i(t) + \tilde{w}_{i,l}(t) + \tilde{h}_{i,l}(t) \tag{2.20}$$

and

$$\tilde{x}_{i,u}(t) = x_i(t-T) + \tilde{f}_i(t) + \tilde{w}_{i,u}(t) + \tilde{h}_{i,u}(t) \tag{2.21}$$

Since $w_l(x) \leq w(x,\tau) \leq w_u(x)$ for any $\tau \in [t-T, t]$ and $\theta_l \leq \theta \leq \theta_u$, it follows that if $\theta_j(\tau) = 0$ for any $\tau \in [t-T, t]$, then the following equation holds:

$$\tilde{x}_{i,l}(t) \leq x_i(t) \leq \tilde{x}_{i,u}(t) \tag{2.22}$$

Therefore, $x_i(t) \neq [\tilde{x}_{i,l}(t), \tilde{x}_{i,u}(t)]$ implies that $\theta_j(\tau) \neq 0$ for some $\tau \in [t-T, t]$.

Part 2: Given $x_i(t) \notin [x_{i,l}(t), x_{i,u}(t)]$, there exists $\tilde{d} > 0$ such that $x_i(t) < x_{i,l}(t) - \tilde{d}$ or $x_i(t) > x_{i,u}(t) + \tilde{d}$. Since θ is bounded, there exists $d' > 0$ such that if $|d_{i,k}(x)| < d'$ over $[t-T, t]$ for all $k \in \{1, \ldots, q\} \backslash \{j\}$, then $\tilde{h}_{i,l}(t) > -\tilde{d}$ and $\tilde{h}_{i,u}(t) < \tilde{d}$. For any $k \in \{1, \ldots, q\} \backslash \{j\}$, since $d_{ik}(\cdot)$ is continuous and $d_{ik}(\tilde{x}) = 0$, there exists $d > 0$ such that $|d_{ik}(x)| < d'$ for any $x \in B_d$. Because $x(t_d) \in D$, it follows from Assumption 2.3 that under the switching rule of Eq. (2.15), there exists $T_c' > 0$ such that $x(t) \in B_d$ for all $t \geq T_c' - T$. Then, for $t \geq T_c'$, we have $\tilde{h}_{i,l}(t) > -\tilde{d}$ and $\tilde{h}_{i,u}(t) < \tilde{d}$. It follows that

$$x_i(t) < x_{i,l}(t) - \tilde{d} < x_{i,l}(t) + \tilde{h}_{i,l}(t) = \tilde{x}_{i,l}(t) \tag{2.23}$$

or

$$x_i(t) > x_{i,u}(t) + \tilde{d} > x_{i,u}(t) + \tilde{h}_{i,u}(t) = \tilde{x}_{i,u}(t) \tag{2.24}$$

which implies that $x_i(t) \notin [\tilde{x}_{i,l}(t), \tilde{x}_{i,u}(t)]$. This completes the proof of Theorem 2.2. □

The relationship between the estimated bounds and the state measurements under normal and faulty conditions are shown in Fig. 2.1. Under normal conditions, the state x_i (denoted by the solid line) is in between the lower bound $\tilde{x}_{i,l}$ and upper bound $\tilde{x}_{i,u}$ (denoted by the dashed lines) at time t (see Fig. 2.1(a)). In the presence of a fault, the bounds may not be tight enough for a fault to be isolated under nominal operation (see Fig. 2.1(b)). At a fault isolation point, however, the bounds become tight so that a fault is isolated (see Fig. 2.1(c)).

Without loss of generality, let $\{1, \ldots, q\}$ be an index set of the states that satisfy the

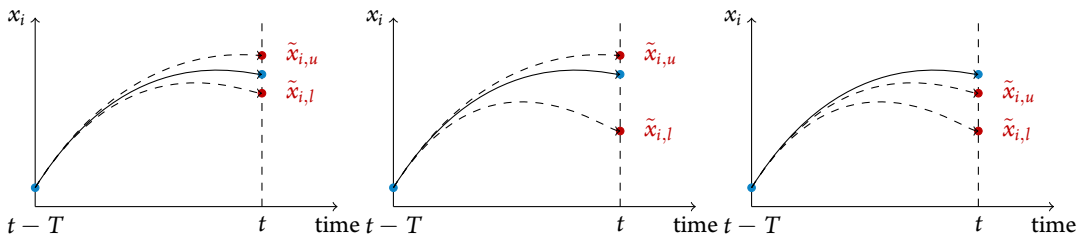

Figure 2.1: Schematic of the relationship between the estimated bounds and the state measurements for x_i (a) under normal conditions, and when the process is (b) under nominal operation and (c) at a fault isolation point in the presence of a fault.

relationship between faults and states at a fault isolation point. Note that each state is associated with a unique fault. The implementation of the active fault isolation scheme of Theorem 2.2, with the use of the robust fault detection design of Theorem 2.1, is illustrated in Fig. 2.2 and proceeds as follows:

1. At time $t_k = k\Delta_{FDI}$, $k = 0, \ldots, \infty$, evaluate thresholds

$$t_{h,i}(k) = \frac{x_{i,u}(t_k) - x_{i,l}(t_k)}{2} \tag{2.25}$$

and residuals

$$r_i(k) = \left| x_i(t_k) - \frac{x_{i,l}(t_k) + x_{i,u}(t_k)}{2} \right| \tag{2.26}$$

for $i = 1, \ldots, n$, according to Eqs. (2.5) and (2.6), where Δ_{FDI} denotes the evaluation period (i.e., the time between two consecutive evaluations).

2. According to Theorem 2.1, if $r_i(k) > t_{h,i}(k)$ for some $i \in \{1, \ldots, n\}$, then a fault is detected, and let $t_d = t_k$ be the time of fault detection if it is the first time that the fault is detected. Note that $x_i(t_k) \notin [x_{i,l}(t_k), x_{i,u}(t_k)]$ iff $r_i(k) > t_{h,i}(k)$.

3. At time t_k, evaluate thresholds

$$\tilde{t}_{h,i}(k) = \frac{\tilde{x}_{i,u}(t_k) - \tilde{x}_{i,l}(t_k)}{2} \tag{2.27}$$

and residuals

$$\tilde{r}_i(k) = \left| x_i(t_k) - \frac{\tilde{x}_{i,l}(t_k) + \tilde{x}_{i,u}(t_k)}{2} \right| \tag{2.28}$$

for $i = 1, \ldots, q$, according to Eqs. (2.20) and (2.21).

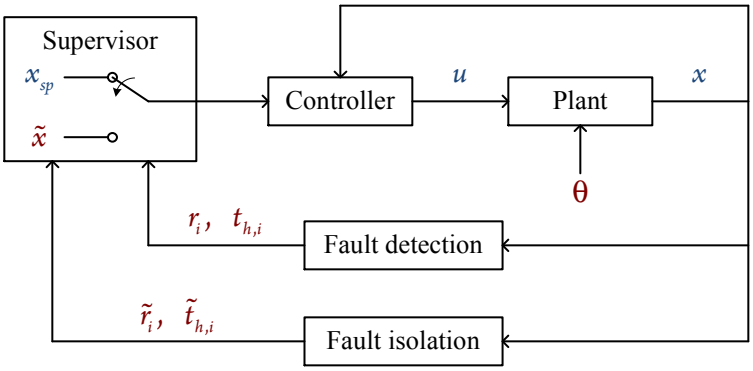

Figure 2.2: Schematic of the active fault isolation scheme. The process is subject to faults denoted by θ. A fault is detected by checking whether some detection residual r_i breaches its threshold $t_{h,i}$. Upon fault detection, the supervisor shifts the control objective from operating the process at the nominal operating point x_{sp} to driving the process to move towards a fault isolation point $\tilde{x}$. A fault is isolated by checking which isolation residual $\tilde{r}_i$ breaches its threshold $\tilde{t}_{h,i}$

4. According to Theorem 2.2, if $\tilde{r}_i(k) > \tilde{t}_{h,i}(k)$, then a fault θ_j for some $j \in \{1, \ldots, q\}$ is isolated, and let t_k be the time of fault isolation. Note that $x_i(t_k) \notin [\tilde{x}_{i,l}(t_k), \tilde{x}_{i,u}(t_k)]$ iff $\tilde{r}_i(k) > \tilde{t}_{h,i}(k)$. Otherwise, go to Step 5.

5. If a fault has been detected (i.e., $t_k \geq t_d$), switch the control law according to Eq. (2.15). Repeat Step 1.

Remark 2.6. The idea of the active fault isolation design in Theorem 2.2 is to move the process to a desired region where the dedicated residuals, denoted by $\tilde{r}_i$, become uniquely sensitive to the complex faults. To this end, a switching rule is designed to, upon fault detection, switch the control objective of operating the process at the nominal equilibrium point to driving it to move towards a fault isolation point. For a given fault, the effect of the other faults on the evolution of the same process state then can be reduced to an insignificant level as the process approaches the fault isolation point (or enters the desired region around that point), while the effect of the fault under consideration can still be retained and reflected. The declaration of this fault is based on a fault detection design by treating other faults as process disturbances. This is achieved by extending the fault detection design of Theorem 2.1. It is also shown in Theorem 2.2 that if the fault can be differentiated from process uncertainty (i.e., $x_i(t) \notin [x_{i,l}(t), x_{i,u}(t)]$), then it can also be isolated (i.e., $x_i(t) \notin [\tilde{x}_{i,l}(t), \tilde{x}_{i,u}(t)]$) as long as the process states are sufficiently close to the fault isolation point (i.e., d is sufficiently small).

Remark 2.7. Note that the active fault isolation scheme of Theorem 2.2 differs from the existing results (e.g., [27]), where fault detection and isolation are achieved simultane-

ously. The class of nonlinear systems studied in [27] naturally are of a favorable structure allowing the generation of dedicated residuals that are sensitive to faults regardless of the region where the process operates. Because the occurrence of one fault is not eclipsed by others, the detection of a fault also indicates the location of the faulty component. As complex faults are concerned, however, the dedicated residuals may not be sensitive to faults in the region where the process operates under nominal operation, losing their ability as isolation indicators. Of course if the current operation allows for isolation of faults (as expected for a well designed process and for most of the "expected" faults), the existing FDI schemes can be used. The applicability of the proposed method is for the "unexpected", which, while triggering the fault detection mechanism (making it obvious that something has gone wrong) might not allow isolation of the fault under nominal operation (determining what exactly has gone wrong). The triggering of the fault isolation mechanism, is therefore, reliant on the "nominal" FDI mechanism, which at least detects that a fault has taken place, and is an independent fault detection design (see also Fig. 2.2) activating the control law for the purpose of fault isolation.

Remark 2.8. The proposed active fault isolation design relies on the ability to drive the process to a fault isolation point and the ability to differentiate between faults and plant-model mismatch. In the presence of input constraints, an explicit characterization of a stability region (see [75] for an example) can be used to ascertain the ability to stabilize the process at a desired operating point from a certain region by treating faults as process disturbances. In addition to bias or drift faults, this method is also applicable to the case where an actuator possibly freezes as long as the remaining functioning actuators can still provide sufficient control action or additional control action is available (e.g., through the use of a backup control actuator) during fault isolation. It should be noted, however, that the purpose of switching the control law is to reduce the possible effect of other faults, but not necessarily to stabilize the process at the fault isolation point. An explicit consideration of plant-model mismatch makes it possible to quantify the effect of uncertainty and other faults on an isolation indicator. Consequently, even before the process approaches the vicinity of the fault isolation point, the location of the fault could be identified (see Section 2.5.1 for an illustration).

Remark 2.9. The idea of active fault isolation can be extended to handle the case where there does not exist a single operating point that can make residuals sensitive to all the faults. For this case, fault isolation can be achieved by moving the process to a series of operating points. To illustrate this, consider a system described by $\dot{x} = f(x) + g(x)u + (x-a)\theta_1 + (x+a)\theta_2$, where $x \in \mathbb{R}$ and $a > 0$. In this example, there does not exist a single point at which the effects of θ_1 and θ_2 on the evolution of the system state can be

simultaneously eliminated. For this system, we can switch the control law to, upon fault detection, sequentially operate the system at point $x = -a$ and $x = a$, at which isolation of faults θ_1 and θ_2 can be carried out, respectively. We also consider a system described by $\dot{x} = f(x) + g(x)u + (x^2 + 1)\theta_1 + \theta_2$, where $x \in \mathbb{R}$. In this example, there does not exist a point at which the effect of θ_1 or θ_2 can be eliminated. To differentiate between their effects, we can operate the system to move away from the origin to amplify the possible effect of θ_1, facilitating isolation of the fault θ_1. Isolating the fault θ_2 will require operation at the origin, at which the effect of θ_1 on the evolution of the state is minimum. The fault θ_2 can only be isolated when its actual effect exceeds the possibly extreme effect of θ_1.

Remark 2.10. Accurate and timely identification of a fault is required to trigger the implementation of active FTC schemes, such as control reconfiguration (see, e.g., [27, 64]) or safe-parking (see, e.g., [74, 85, 86]), as a prerequisite. In the case of control reconfiguration, a backup control configuration that does not use the failed actuator is used to preserve nominal operation. If backup control actuators are not available, safe-parking techniques can be used to operate the process at an appropriate temporary operating point (which is referred to as a safe-parking point), starting from where nominal operation is resumed upon fault repair. To implement these fault-handling methods, information on the location of faults is needed to choose an appropriate backup control configuration or a safe-park point. Without the ability to isolate complex faults, however, the aforementioned fault-handling techniques may not be able to deal with faults effectively.

2.5 Simulation Examples

In this section, we first illustrate the proposed fault isolation design through a chemical reactor example, and then demonstrate its applicability through the solution copolymerization process in Section 2.3.

2.5.1 Illustrative Simulation Example

In this section, we consider a CSTR example, where an irreversible elementary exothermic reaction of the form $A \xrightarrow{k} B$ takes place. The feed to the reactor is composed of two streams, as shown in Fig. 2.3. One stream consists of reactant A at a flow rate F_1, concentration C_{A1}, temperature T_1, and F_1 is adjustable. The other consists of reactant A at a flow rate F_2, concentration C_{A2}, temperature T_2, and F_2 is fixed under fault-free conditions. A cooling jacket is equipped to remove heat from the reactor. The cooling stream going to

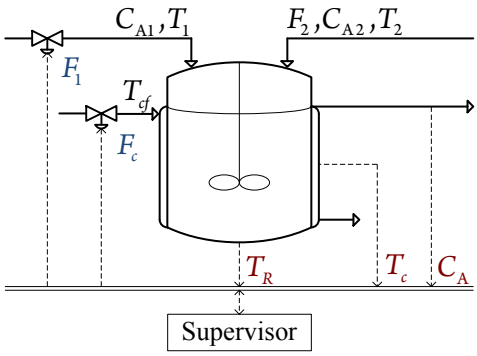

Figure 2.3: Schematic of the chemical reactor example of Section 2.5.1.

the jacket is at a flow rate F_c and temperature T_{cf}. The mathematical model of this chemical reactor takes the following form:

$$\begin{aligned}
\dot{C}_A &= \sum_{i=1}^{2} \frac{F_i}{V}(C_{Ai} - C_A) - k_0 e^{-E/RT_R} C_A \\
\dot{T}_R &= \sum_{i=1}^{2} \frac{F_i}{V}(T_i - T_R) + \frac{(-\Delta H)}{\rho c_p} k_0 e^{-E/RT_R} C_A - \frac{UA}{\rho c_p V}(T_R - T_c) \\
\dot{T}_c &= \frac{F_c}{V_c}(T_{cf} - T_c) + \frac{UA}{\rho_c c_{pc} V_c}(T_R - T_c)
\end{aligned} \tag{2.29}$$

where C_A is the concentration of species A, T_R is the temperature in the reactor, T_c is the temperature in the cooling jacket, V is the volume of the reactor, k_0, E, and ΔH are the pre-exponential constant, the activation energy, and the enthalpy of the reaction, respectively, R is the ideal gas constant, ρ and c_p are the density and the heat capacity of the fluid in the reactor, respectively, U is the overall heat transfer coefficient, A is the heat transfer area of the CSTR, V_c is the volume of the cooling jacket, and ρ_c and c_{pc} are the density and the heat capacity of the cooling stream, respectively. The process parameters can be found in Table 2.2.

The control objective under fault free conditions is to stabilize the process at the nominal equilibrium point $C_A = 0.5$ mol/L, $T_R = 350$ K, and $T_c = 345$ K by manipulating $u = [F_1, F_c]^T$, where $0 \leq F_1 \leq 150$ L/min and $0 \leq F_c \leq 10$ L/min. The corresponding steady-state values of the input variables are $F_1 = 21.75$ L/min and $F_c = 1.14$ L/min. A Lyapunov-based predictive controller of [75] is used as one example of the robust control design to illustrate the implementation of the proposed method. The hold-time for the control action is chosen as $\Delta = 0.25$ min, the prediction horizon is chosen as 2Δ, the weighting matrices used to penalize the deviations of the state and input from their nom-

Table 2.2: Process parameters for the chemical reactor example of Section 2.5.1.

Parameter	Value	Unit
F_2	115.90	L/min
V	100	L
k_0	7.2×10^{10}	min^{-1}
E/R	8750	K
ΔH	-5×10^2	J/mol
ρ	1000	g/L
c_p	0.239	J/g·K
UA	5×10^4	J/min·K
V_c	20	L
ρ_c	1000	g/L
c_{pc}	4.2	J/g·K
C_{A1}	1.2	mol/L
C_{A2}	0.8	mol/L
T_1	340	K
T_2	360	K
T_{cf}	293	K

inal values are chosen as $Q_w = \text{diag}[10^5, 10^3, 10]$ and $R_w = \text{diag}[20, 100]$, respectively, and a quadratic Lyapunov function $V = x^{\text{T}}Px$ is used.

Consider the process of Eq. (2.29) subject to actuator faults in F_1 and F_c, and a process fault in F_2; that is, the fault vector $\theta(t) = [\tilde{F}_1, \tilde{F}_2, \tilde{F}_c]^{\text{T}}$, where the tilde denotes faults. It follows that

$$D(x) = \begin{bmatrix} \frac{C_{A1}-C_A}{V} & \frac{C_{A2}-C_A}{V} & 0 \\ \frac{T_1-T_R}{V} & \frac{T_2-T_R}{V} & 0 \\ 0 & 0 & \frac{T_{cf}-Tc}{V_c} \end{bmatrix} \tag{2.30}$$

According to Definition 2.1, the system has a fault isolation point $\tilde{x} = [C_{A2}, T_1, T_c]^{\text{T}}$, with $C_A = 0.8$ mol/L, $T_R = 340$ K, and $T_c = 328.5$ K. The corresponding steady-state values of the inputs are $F_1 = 95.87$ L/min and $F_c = 3.84$ L/min. The bounds on uncertain variables used in the FDI design are $\pm 5\%$ for k_0 and -10% and 5% for UA. The faults are bounded as $-20 \leq \tilde{F}_i \leq 20$ L/min, $i = 1, 2$. The fault detection horizon $T' = 2\Delta$, and the evaluation period $\Delta_{FDI} = \Delta/10$.

To illustrate the active fault isolation design for the system of Eq. (2.29) subject to plant-model mismatch, we consider a fault that takes place in the actuator used to adjust F_1

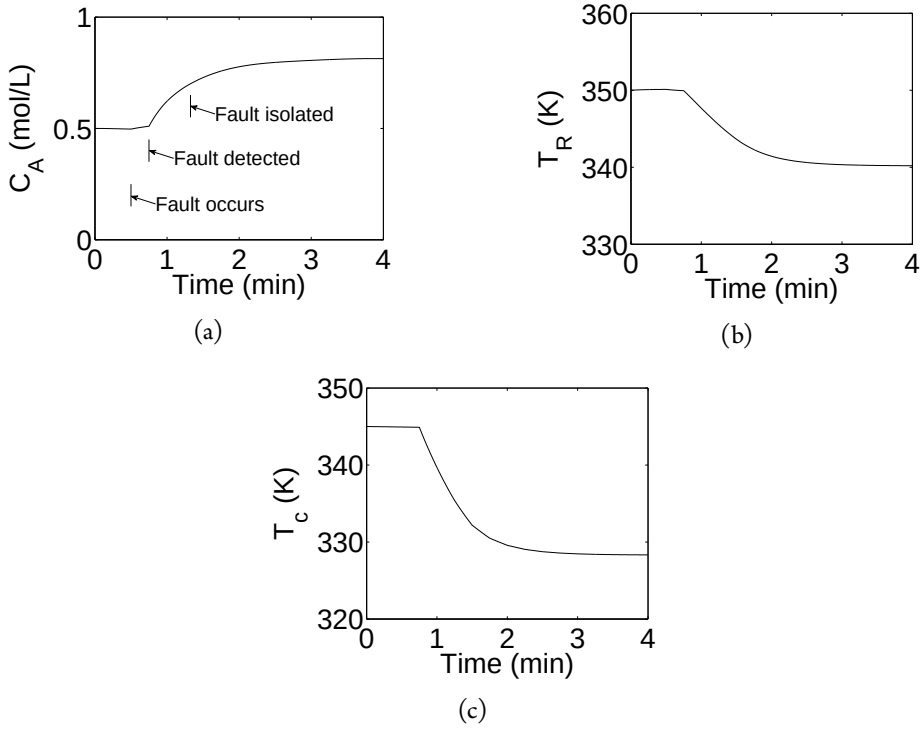

Figure 2.4: Closed-loop state profiles for the chemical reactor example.

at time $t_f = 0.5$ min. Specifically, the fault is described as follows:

$$\tilde{F}_1 = \begin{cases} 0, & \text{if } 0 \leq t < t_f \\ 10, & \text{if } t \geq t_f \end{cases} \tag{2.31}$$

Furthermore, k_0 is 2% larger than its nominal value and UA is 5% smaller than its nominal value. The process starts from the nominal equilibrium point. The closed-loop state profiles with the implementation of the proposed active fault isolation design are shown in Fig. 2.4, where the times of fault occurrence, detection, and isolation are also indicated. It can be seen that the fault is isolated even before the process states approach the vicinity of the fault isolation point. The corresponding prescribed and actual input profiles are shown by the solid and dashed lines, respectively, in Fig. 2.5.

To detect faults, the residuals r_i, i =1, 2, 3, and the corresponding thresholds for the purpose of fault detection are generated, as shown by the solid and dashed lines, respectively, in Fig. 2.6. It is observed that r_1 breaches its threshold at time 0.75 min, indicating the occurrence of a fault. Because r_1 is associated with faults in F_1 and F_2, it is only concluded that a fault takes place in F_1 or F_2. Note that r_2 does not breach its threshold because

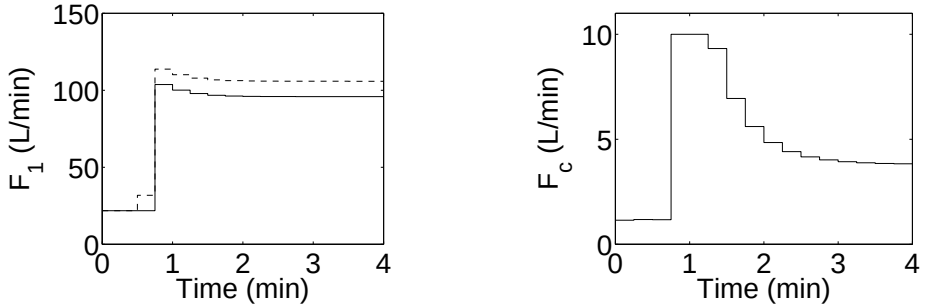

Figure 2.5: Prescribed (solid lines) and actual (dashed lines) input profiles for the chemical reactor example.

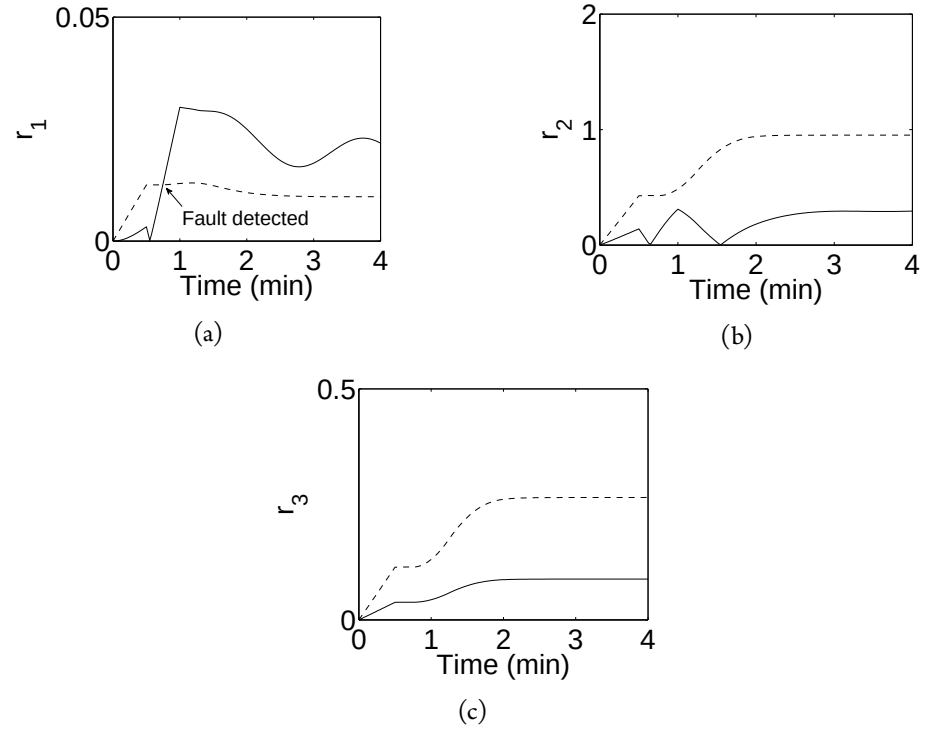

Figure 2.6: Residuals (solid lines) and thresholds (dashed lines) for detecting faults in the chemical reactor example. A fault is detected at 0.75 min via r_1 breaching its threshold.

the fault and uncertainty counteract the effect of each other in this specific example. Note also that r_3 serves as a dedicated residual for F_c.

To isolate faults, the supervisor dictates switching the controller to drive the process to move towards the fault isolation point $\tilde{x}$. The residuals $\tilde{r}_1$ and $\tilde{r}_2$ and the correspond-

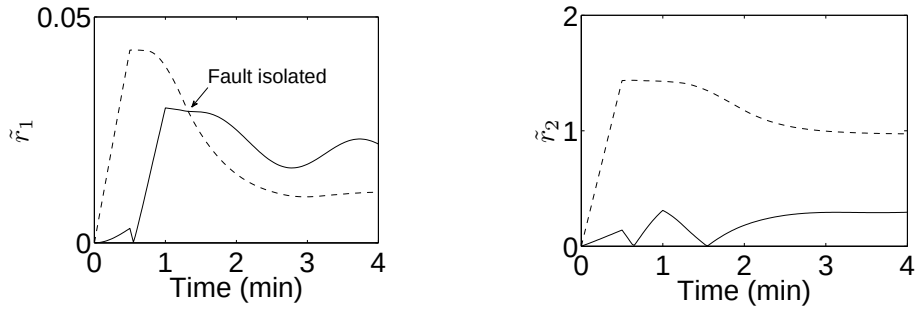

Figure 2.7: Residuals (solid lines) and thresholds (dashed lines) for isolating faults in the chemical reactor example in the presence of the active fault isolation scheme. A fault in F_1 is isolated at 1.325 min via $\tilde{r}_1$ breaching its threshold.

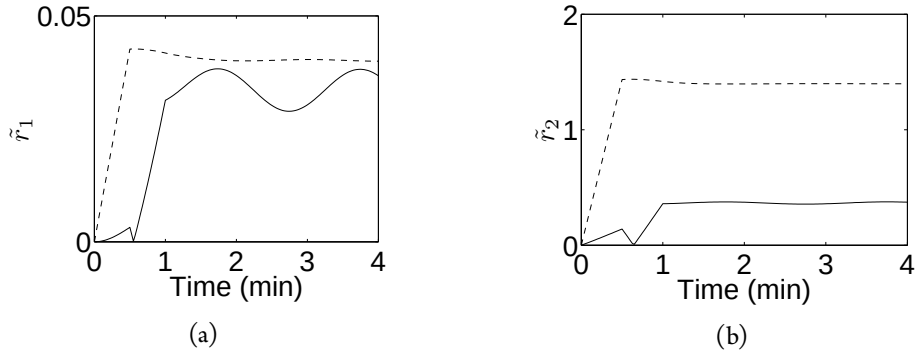

Figure 2.8: Residuals (solid lines) and thresholds (dashed lines) for isolating faults in the chemical reactor example under nominal operation. The residuals are not sufficiently sensitive to faults in the absence of the active fault isolation scheme.

ing thresholds for the purpose of fault isolation are shown by the solid and dashed lines, respectively, in Fig. 2.7. It can be seen that before the switching, $\tilde{r}_1$ and $\tilde{r}_2$ are below their thresholds, and after the switching, both the thresholds decrease as the process approaches the fault isolation point. Furthermore, $\tilde{r}_1$ breaches its threshold at time 1.325 min, indicating the occurrence of a fault in F_1. Although they are dedicated residuals, $\tilde{r}_1$ and $\tilde{r}_2$ are not sufficiently sensitive to faults (i.e., the residuals are below the thresholds) under nominal operation, as shown in Fig. 2.8. In contrast, they become sensitive to faults after the switching in the presence of the proposed active fault isolation scheme, as shown in Fig. 2.7.

2.5.2 Application to the Solution Copolymerization Reactor

In this section, we demonstrate the effectiveness of the proposed method via the process example introduced in Section 2.3. In addition to parametric uncertainty, this method can explicitly handle the "normal" process disturbances (those that are not treated as faults) as long as they can be captured by the uncertainty term in the process description of Eq. (2.1). As the presence of general process disturbances and measurement noise are concerned, the computed thresholds can be appropriately relaxed to improve the performance of the method. In particular, the thresholds should not be too small in order to maintain a low rate of false alarms. The choice of thresholds satisfying this requirement can be made using the normal plant operating data. Besides, they should not be too large to lose sensitivity to faults. The choice of thresholds satisfying this requirement can be made using process data on past faults or simulation data. For a well designed process, the faults that do not lead to residuals breaching the thresholds would likely have small magnitudes, and would not significantly affect the process evolution immediately. As the magnitude of a fault increases and its effect exceeds that of disturbances and noise on the value of the residual, the proposed method can effectively declare the occurrence and location of the fault. A study on how to generate optimal residuals (possibly using the known probabilistic distribution functions of disturbances and noise) is outside the scope of this work, and remains a challenging problem for nonlinear process systems.

We first show that faults may not be isolated under nominal operation. At the nominal operating point, the fault distribution matrix normalized for each row is evaluated as follows:

$$D = \begin{bmatrix} 0.9982 & -0.0297 & -0.0297 & -0.0297 & -0.0297 & 0 \\ -0.4682 & 0.3507 & -0.4682 & -0.4682 & -0.4682 & 0 \\ -0.0004 & -0.0004 & 1.0000 & -0.0004 & -0.0004 & 0 \\ -0.2723 & -0.2723 & -0.2723 & 0.8387 & -0.2723 & 0 \\ -0.0187 & -0.0187 & -0.0187 & -0.0187 & 0.9993 & 0 \\ 0.0054 & 0.0054 & 0.0054 & 0.0054 & 0.0054 & 0.9999 \end{bmatrix} \tag{2.32}$$

It can be seen that the element in the first row and first column is approximately equal to one, which is much larger than the others in the same row. This implies that the effect of the fault in Q_a on the evolution of C_a is much more significant compared to the others. Therefore, we use the differential equation for C_a to generate the residual $\tilde{r}_1$ as an isolation indicator, which should be sensitive to this fault under nominal operation. Similarly, residuals $\tilde{r}_3$, $\tilde{r}_5$, and $\tilde{r}_6$ are generated using the differential equations for C_i, C_t, and T_R for faults

in Q_i, Q_t, and T_c, respectively. Note that the differences between the element in row 2 (row 4) and column 2 (column 4), and other elements in the same row are not significant compared to other rows in the fault distribution matrix of Eq. (2.32). Therefore, the isolation residuals designed for faults in Q_b and Q_s using the differential equations for C_b and C_s may not be enough sensitive to those faults under nominal operation. To show this point, we consider a fault taking place in Q_b at time $t_f = 40$ hr, which is described by

$$\theta_2 = \begin{cases} 0, & \text{if } 0 \leq t < t_f \\ -15\left[1 - e^{-2(t-t_f)}\right], & \text{if } t \geq t_f \end{cases} \tag{2.33}$$

It can be seen from Figs. 2.9 and 2.10 that the process states sill remain around the nominal operating point after the fault takes place, with inputs deviating from where they were before the fault occurrence. The fault detection residuals $r_j, j = 1, \ldots, 6$, are generated using the corresponding differential equations. To reduce false alarms caused by measurement noise, a fault is declared only when 90% of the residual values breach the corresponding threshold for 20 successive evaluations. Because measurement noise affects the residual r_5 much more than uncertainty, this residual is relaxed by 0.01 to reduce false alarms. As shown in Fig. 2.11, the fault is first detected at time $t_d = 44$ hr through r_5 breaching its threshold. In addition, residuals r_2 and r_4 also breach their thresholds. However, none of the isolation residuals breach their thresholds, as shown in Fig. 2.12. This is because the effects of faults in Q_b and other inputs cannot be well differentiated under nominal operation as explained earlier.

We next show that the fault considered earlier can be isolated through active fault isolation for the solution copolymerization reactor. It can be seen from Eq. (2.14) that to amplify the effect of the fault in Q_b on the evolution of C_b, one can operate the process at a point where C_b is much smaller than its nominal value. To this end, we decrease the flow rate of monomer B to 15 kg/h and increase the flow rate of solvent to 60 kg/h at steady state, respectively, while keeping the others unchanged. This leads to an operating point at which $C_a = 4.340 \times 10^{-1}$ kmol/m^3, $C_b = 1.457$ kmol/m^3, $C_i = 3.340 \times 10^{-3}$ kmol/m^3, $C_s = 7.042$ kmol/m^3, $C_t = 5.610 \times 10^{-1}$ kmol/m^3, and $T_R = 346.1$ K. At this operating

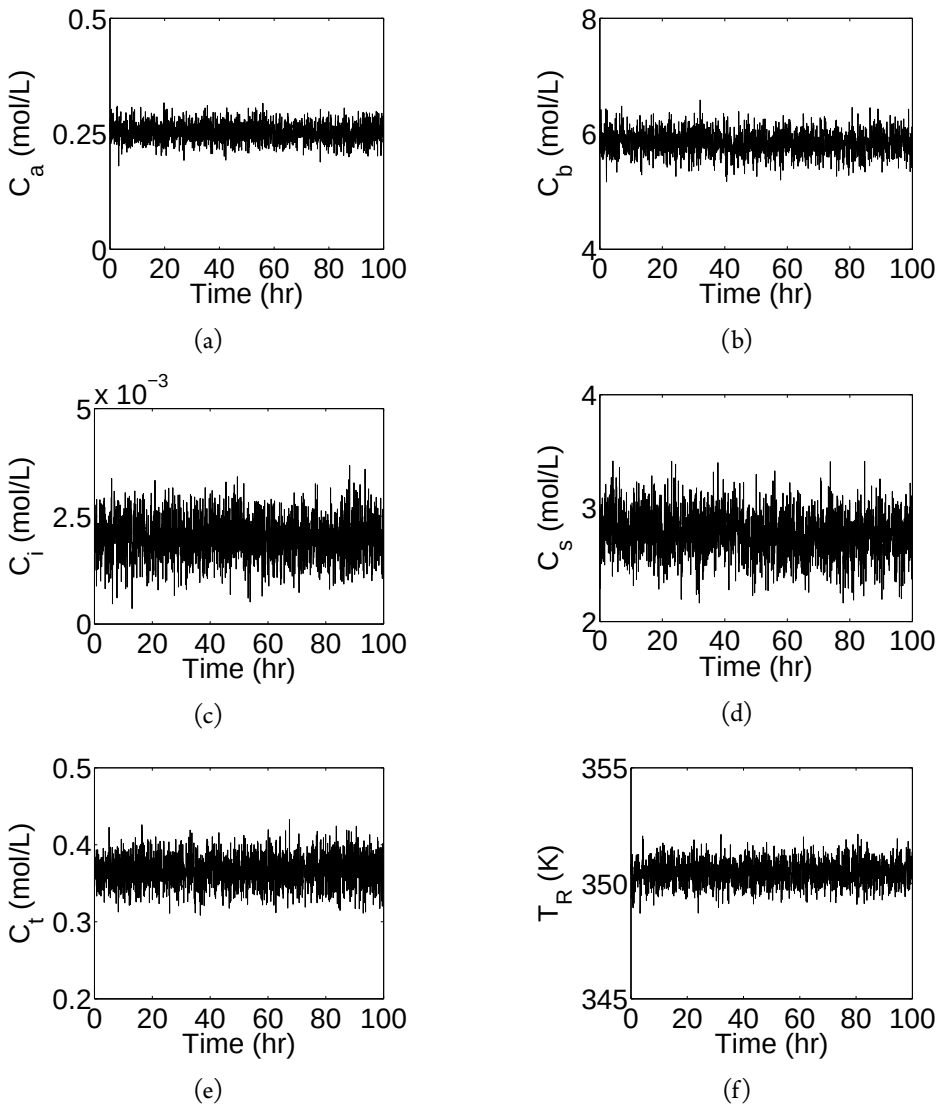

Figure 2.9: State trajectories for the solution copolymerization reactor in the absence of active fault isolation. The process states evolve around the nominal operating point even after the fault takes place.

point, the fault distribution matrix is evaluated as follows:

$$D = \begin{bmatrix} 0.9946 & -0.0517 & -0.0517 & -0.0517 & -0.0517 & 0 \\ -0.1579 & 0.9488 & -0.1579 & -0.1579 & -0.1579 & 0 \\ -0.0006 & -0.0006 & 1.0000 & -0.0006 & -0.0006 & 0 \\ -0.4790 & -0.4790 & -0.4790 & 0.2865 & -0.4790 & 0 \\ -0.0289 & -0.0289 & -0.0289 & -0.0289 & 0.9983 & 0 \\ 0.0144 & 0.0144 & 0.0144 & 0.0144 & 0.0144 & 0.9995 \end{bmatrix} \tag{2.34}$$

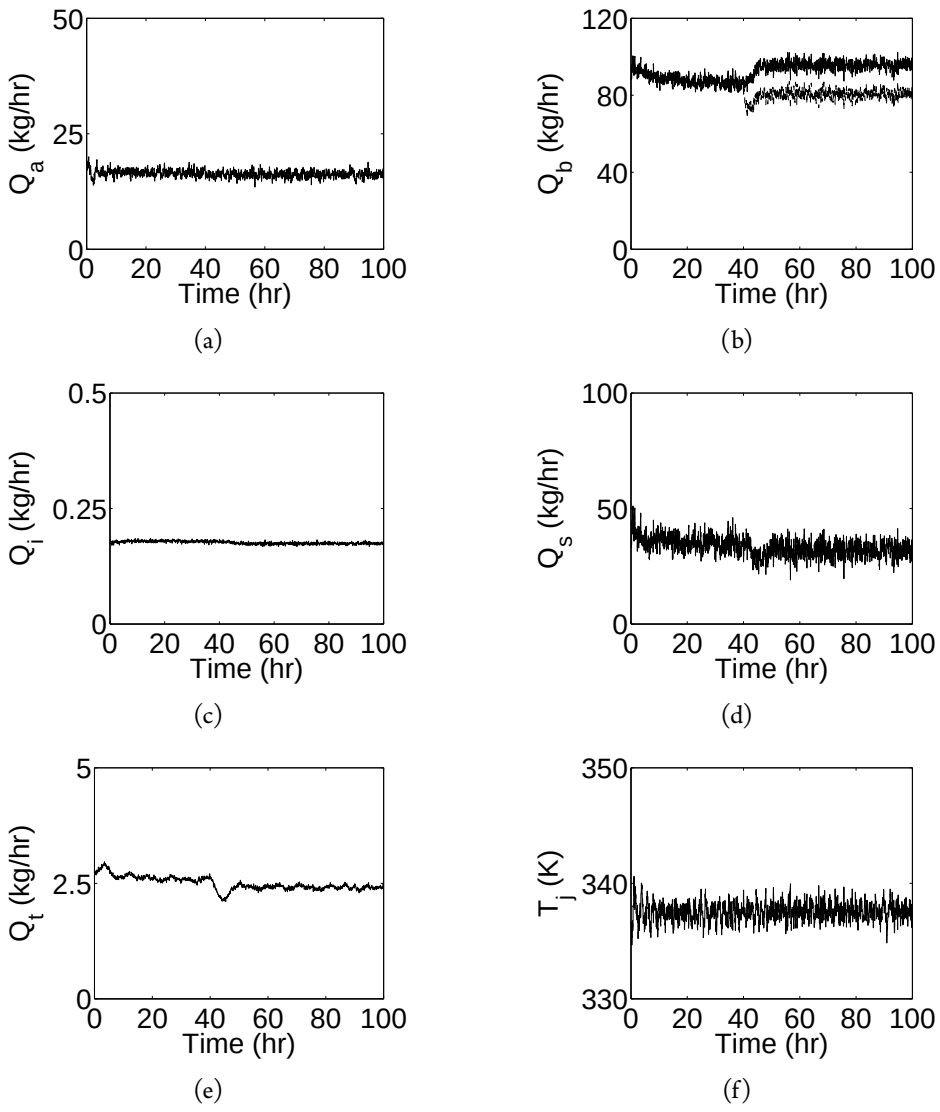

Figure 2.10: Prescribed (solid lines) and actual (dashed line) input trajectories for the solution copolymerization reactor in the absence of active fault isolation. A fault takes place in Q_b at time $t_f = 40$ hr.

It can be seen that the element in row 2 and column 2 is much larger compared to others in the same row. This implies that at this point, the corresponding residual should be more sensitive to the fault in Q_b than at the nominal operating point. For this case, the state and input trajectories are plotted in Figs 2.13 and 2.14, respectively. The fault is first detected at time $t_d = 43.65$ hr through r_5 breaching its threshold, as shown in Fig. 2.15. Upon fault detection, the controller is switched to drive the process to move towards the aforementioned operating point. As the process approaches the desired operating point,

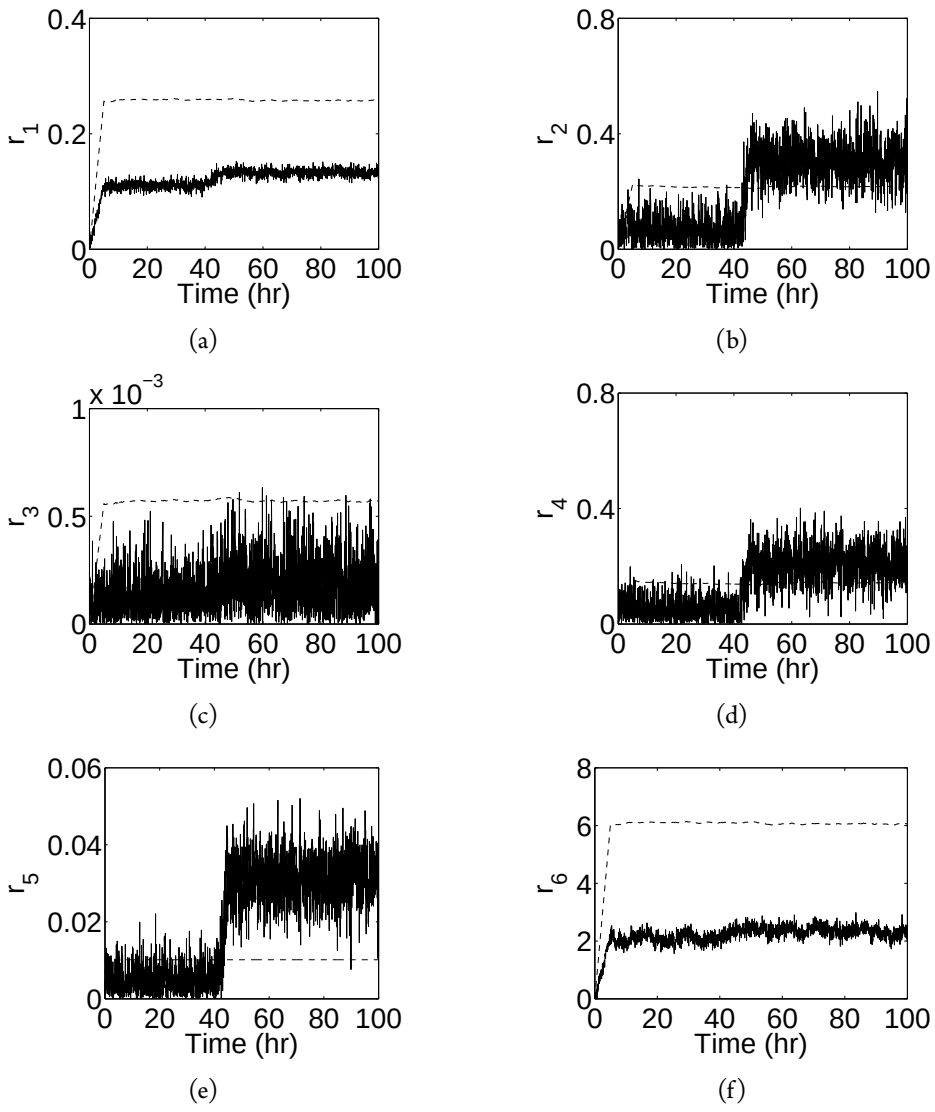

Figure 2.11: Detection residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the absence of active fault isolation. The fault is successfully detected at time $t_d = 44$ hr via r_5 breaching their thresholds.

the threshold for the fault in Q_b decreases (see Fig. 2.16). Consequently, the residual $\tilde{r}_2$ becomes sensitive to the fault, and the fault is successfully isolated at time $t_i = 54.25$ hr via $\tilde{r}_2$ breaching its threshold. If no faults were isolated, the supervisor would subsequently dictate operating the process at a point that favors isolation of a fault in Q_s by following the same idea as illustrated above.

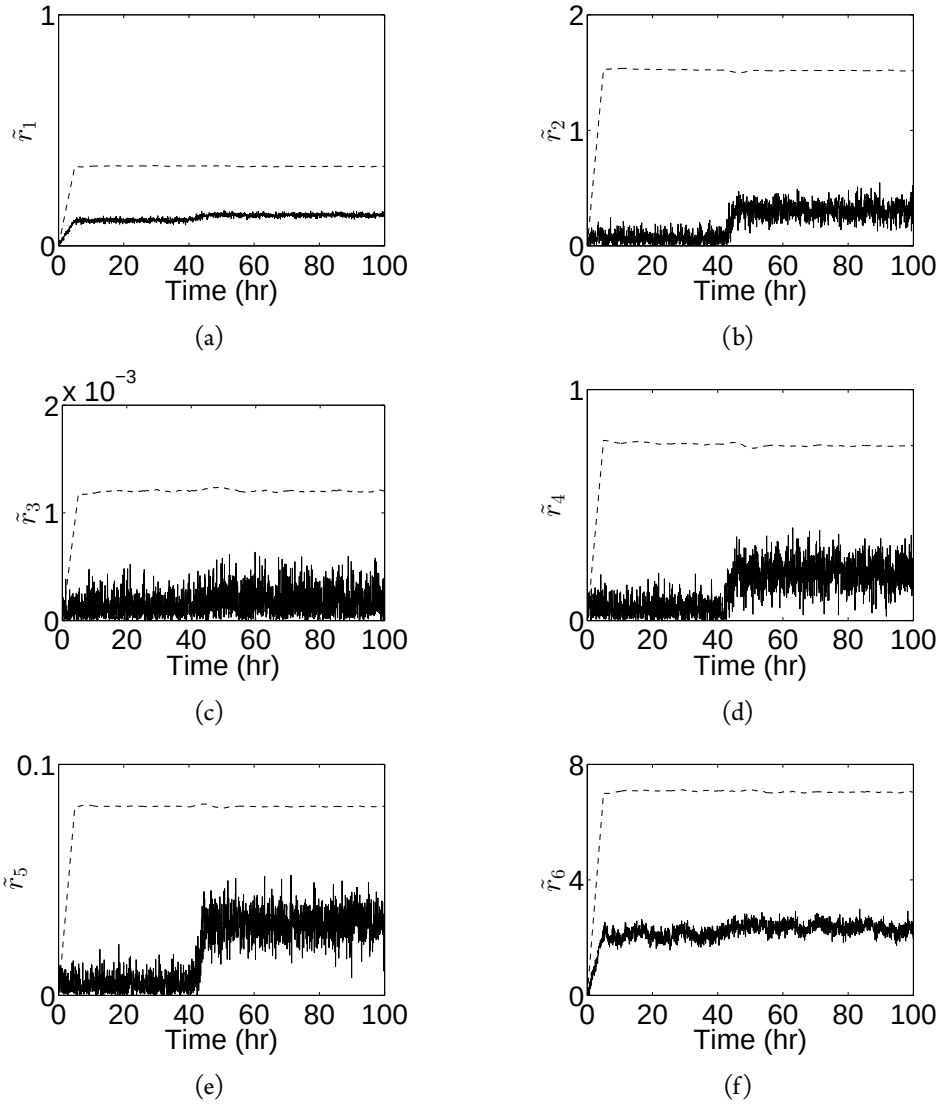

Figure 2.12: Isolation residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the absence of active fault isolation. The residual $\tilde{r}_2$ is not sufficiently sensitive to the fault under nominal operation.

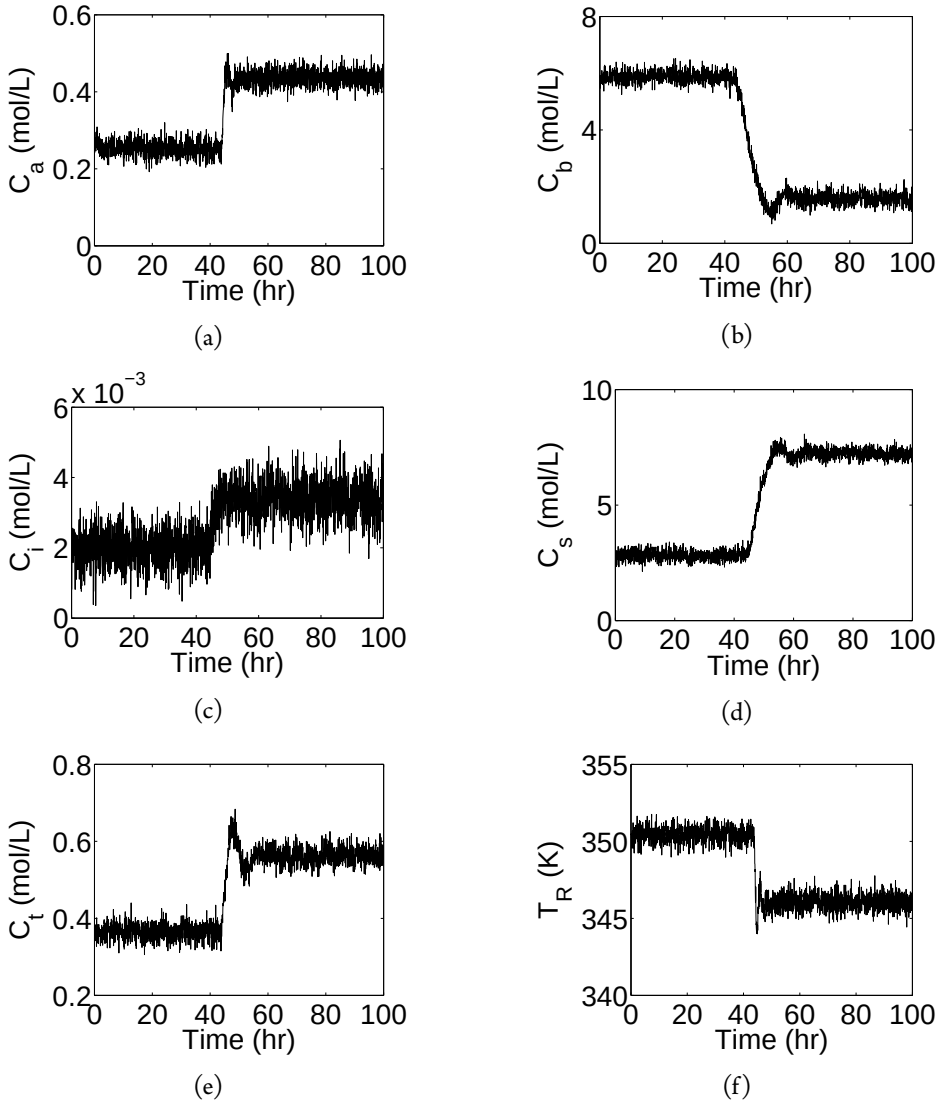

Figure 2.13: State trajectories for the solution copolymerization reactor in the presence of active fault isolation. The process is driven to move towards a point that facilitates isolation of a fault in Q_b upon fault detection at time $t_d = 43.65$ hr.

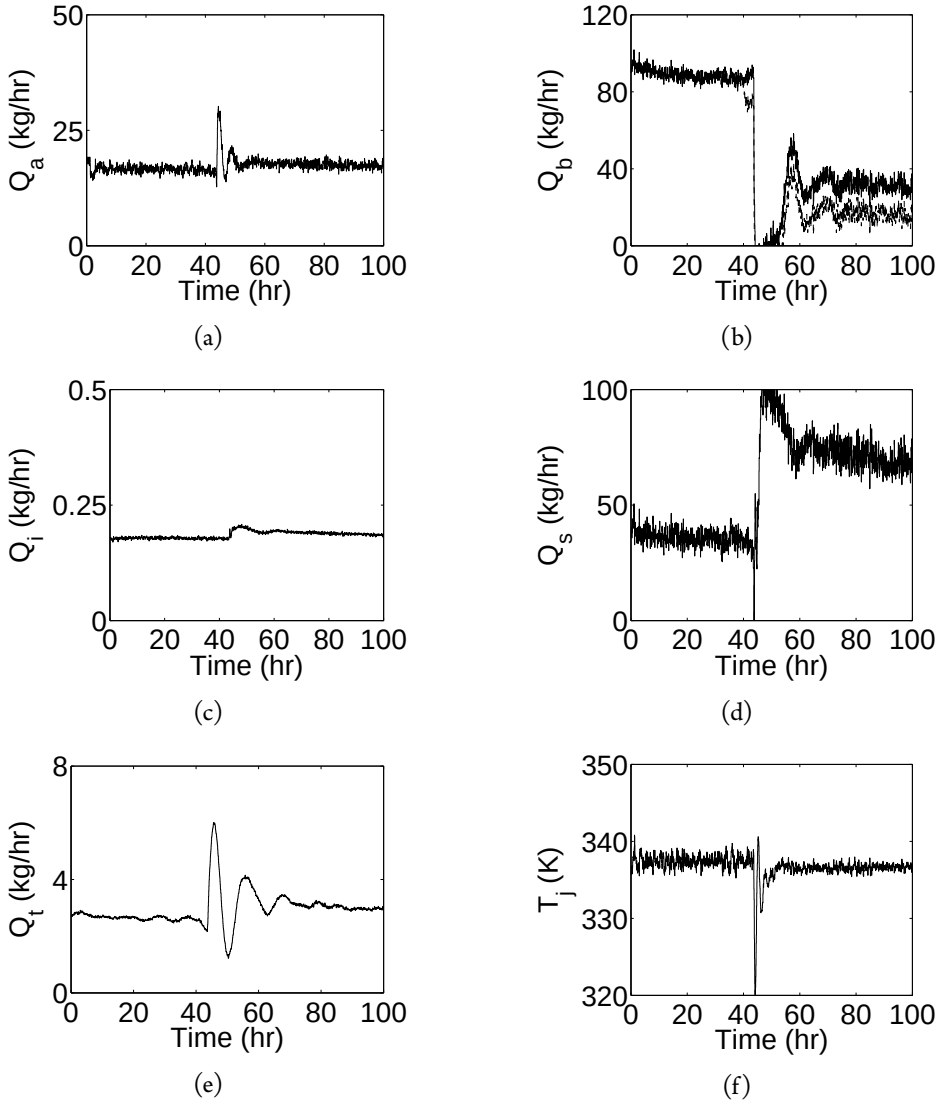

Figure 2.14: Prescribed (solid lines) and actual (dashed line) input trajectories for the solution copolymerization reactor in the presence of active fault isolation. A fault takes place in Q_b at time $t_f = 40$ hr.

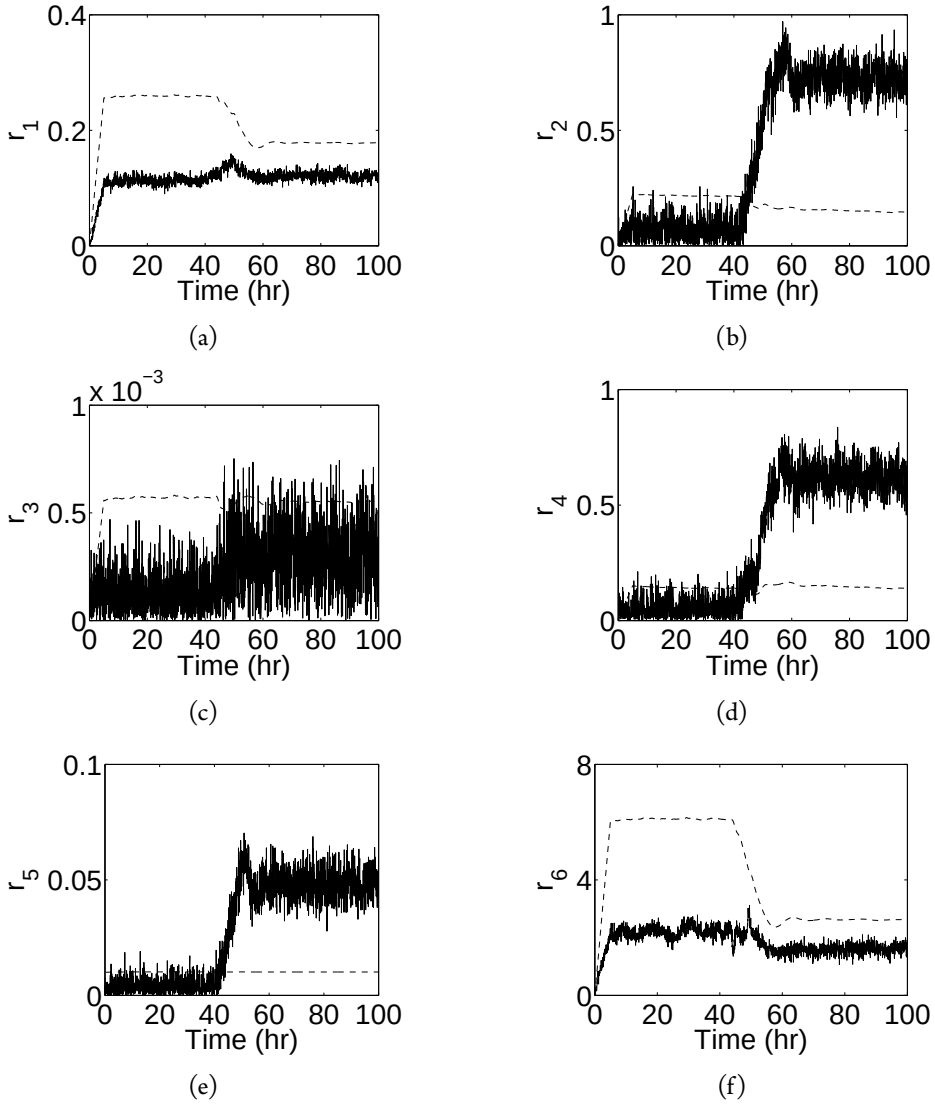

Figure 2.15: Detection residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the presence of active fault isolation. Faults are successfully detected at time $t_d = 43.65$ hr via r_5 breaching its threshold.

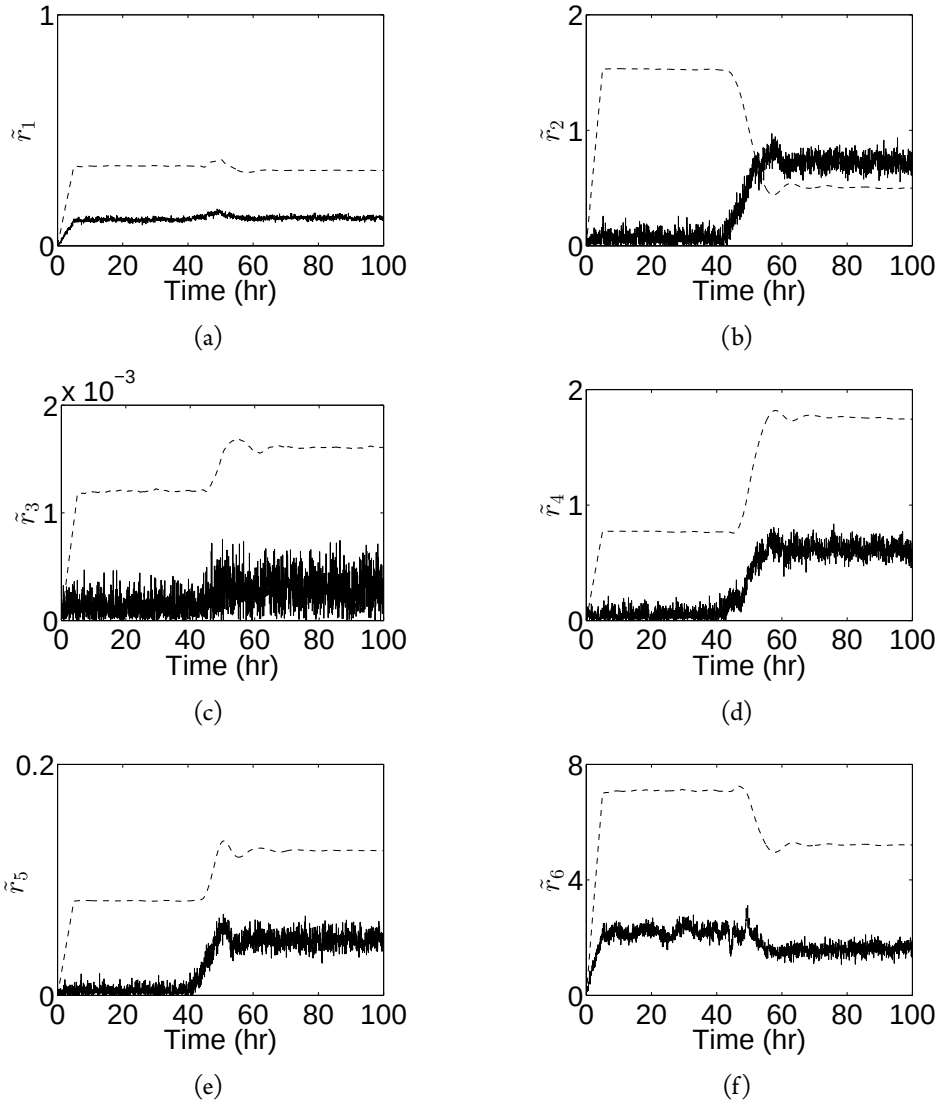

Figure 2.16: Isolation residuals (solid lines) and thresholds (dashed lines) for the solution copolymerization reactor in the presence of active fault isolation. The fault is isolated at time $t_i = 54.25$ hr via $\tilde{r}_2$ breaching its threshold.

2.6 Conclusions

This chapter considered the problem of designing an active fault isolation scheme for nonlinear process systems subject to uncertainty. The faults under consideration include bounded actuator faults and process disturbances that directly affect the evolution of the same process states. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory control. To this end, a dedicated fault isolation residual and its time-varying threshold were generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. These residuals, however, may not be sensitive to faults under nominal operation. To make these residuals sensitive to faults, a switching rule was designed to drive the process states, upon detection of a fault using any fault detection methods, to move towards an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea was then generalized to sequentially operate the process at multiple operating points that facilitate isolation of different faults. The effectiveness of the proposed active fault isolation scheme was illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization of MMA and AVc.

Chapter 3

Isolation and Handling of Sensor Faults in Nonlinear Process Systems[1]

3.1 Introduction

The previous chapter has considered the problem of active isolation of actuator faults. In addition to actuator faults, a process control system is subject to abnormalities in measurement sensors. The problem of sensor FDI has been studied extensively for linear systems (see [6] for a survey) by using a bank of Luenberger observers [12], unknown input observers [16], sliding mode observers [89, 90], and subspace identification models [20, 91]. These approaches, however, may not remain effective for nonlinear process systems.

As sensor faults are concerned, observers are typically required to fully or partly recover the system state. The design of observers, however, is a challenging problem for nonlinear process systems, which is often studied in the context of output feedback control due to the non-validity of the separation principle. In this area, high-gain observers are known to have good convergence properties and have been studied for continuous-time systems (e.g., [75, 92, 93]) and sampled-data systems with uniform measurement sampling and control update rates [94] and faster measurement sampling rate than the control update

[1] The results in this chapter have been published in or submitted to:

a. M. Du and P. Mhaskar. Isolation and handling of sensor faults in nonlinear systems. In *Proceedings of the 2012 American Control Conference*, pages 6661–6666, Montréal, Canada, 2012.

b. M. Du and P. Mhaskar. Isolation and handling of sensor faults in nonlinear systems. *Automatica*, submitted on June 5, 2012.

rate [95], typically exploiting a required system structure. In [96], a high-gain observer is coupled with MPC, where the discrete nature of the control implementation is exploited to generalize the class of nonlinear systems to which high-gain observers can be applied. This generalization, however, is developed under the assumption of locally Lipschitz continuity of the control input in the system state, which is difficult to verify due to the implicit nature of MPC. In comparison, one of the contributions of the present work is to generalize the design and applicability of the high-gain observers under an alternate assumption that is easier to verify (the satisfaction of course being case specific; see Remark 3.1).

Compared to actuator faults, relatively fewer results are available for sensor FDI of nonlinear process systems. This problem has been studied for Lipschitz nonlinear systems (see, e.g., [24, 97–100]). In [98], a nonlinear state observer is designed to generate state estimates by using a single sensor. The fault isolation logic, however, is limited to systems with three or more outputs. The method developed in [24, 100] utilizes adaptive estimation techniques to deal with unstructured but bounded uncertainty for FDI, which requires knowledge of Lipschitz constants in the generation of the thresholds. A bank of fault isolation estimators are activated after the detection of a fault, and fault mismatch functions are used to describe the faults that are isolable. The sensor fault estimation problem has been studied in [99], where linear matrix inequality techniques are used to design an observer for the identification of the fault vector. In addition, a sliding mode observer is designed to reconstruct or estimate faults by transforming sensor faults into pseudo-actuator faults in [101]. This approach, however, requires a special system structure, and there is a limitation on system nonlinearity that can be handled. While a bank of observers is used to isolate sensor faults in [102], the observer gain is obtained through the first order approximation of the nonlinear dynamics. Therefore, the performance of the FDI design is subject to the type of nonlinearities. In addition to sensor bias faults, the effect of intermittent unavailability of measurements has also been studied (see, e.g., [65, 94]). In these results, it is shown that stability of the closed-loop system can be established if the maximum time without sensor data losses is small enough. In the case of complete sensor failures, the control reconfiguration-based approach is used to determine which backup configuration is able to preserve closed-loop stability based on the stability region and the maximum allowable data loss that preserves closed-loop stability for the corresponding configuration [65]. In summary, the problem of sensor FDI and FTC stands to gain from further results on designs that explicitly consider process nonlinearity in the detection, isolation, and handling mechanism design.

Motivated by the above considerations, this chapter considers the problem of sensor fault isolation and fault-tolerant control for nonlinear process systems subject to input con-

straints. The key idea of the proposed method is to exploit model-based sensor redundancy through state observer design. To this end, a high-gain observer is first presented and the stability property of the closed-loop system is rigorously established. By exploiting the enhanced applicability of the observer design, a fault isolation scheme is then proposed, which consists of a bank of observers, with each driven by a subset of the measured outputs. The residuals are defined as the discrepancies between the state estimates and their expected trajectories. A fault is isolated when all the residuals breach their thresholds except for the one that is generated without using measurements from the faulty sensor. While there are other results that use the idea of a bank of observers in the context of linear (or linear approximations of nonlinear) systems, the present results provide a rigorous detection and isolation mechanism design and analysis that explicitly handles the presence of nonlinearity and input constraints. After the fault is isolated, the state estimate generated using measurements from the healthy sensors is used in closed-loop to continue nominal operation. The implementation of the proposed method subject to uncertainty and measurement noise is illustrated using a chemical reactor example.

The remainder of this chapter is organized as follows. The process description and a high-gain observer design are presented in Section 3.2. The stability property of the closed-loop system is established in Section 3.3. The fault isolation and handling scheme is proposed in Section 3.4. The simulation results are presented in Section 3.5. Finally, Section 3.6 gives some concluding remarks.

3.2 Preliminaries

Consider a multi-input multi-output nonlinear system described by

$$\begin{aligned} \dot{x} &= f(x) + G(x)u \\ y &= h(x) + \tilde{y} \end{aligned} \tag{3.1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $u \in \mathbb{R}^m$ denotes the vector of constrained input variables, taking values in a nonempty compact convex set $\mathcal{U} \subseteq \mathbb{R}^m$ that contains 0, $y = [y_1, \ldots, y_p]^{\mathrm{T}} \in \mathbb{R}^p$ denotes the vector of output variables, $\tilde{y} = [\tilde{y}_1, \ldots, \tilde{y}_p]^{\mathrm{T}} \in \mathbb{R}^p$ denotes the fault vector for the sensors, and $G(x) = [g_1(x), \ldots, g_m(x)]$. Throughout the thesis, $L_f h(\cdot)$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to a vector function $f(\cdot)$, and $\| \cdot \|$ denotes the Euclidean norm. In the control design, we consider the system of Eq. (3.1) under fault-free conditions (i.e, $\nu \equiv 0$), which satisfies

Assumption 3.1 below.

Assumption 3.1. The functions $f : \mathbb{R}^n \to \mathbb{R}^n$ and $g_i : \mathbb{R}^n \to \mathbb{R}^n$, $i = 1, \ldots, m$, are $\mathcal{C}^1$ functions on their domains of definition, $f(0) = 0$, and the function $h : \mathbb{R}^n \to \mathbb{R}^p$ is smooth on its domain of definition.

Instead of using a specific control design, the results in this chapter are developed for any control law that satisfies Assumption 3.2 below.

Assumption 3.2. For the system of Eq. (3.1), there exists a positive definite $\mathcal{C}^2$ function $V : \mathbb{R}^n \to \mathbb{R}$ such that for any $x \in \Omega_c := \{x \in \mathbb{R}^n : V(x) \leq c\}$, where c is a positive real number, the following inequality holds:

$$L_f V(x) + L_G V(x) u_c(x) \leq -\alpha(V(x)) \tag{3.2}$$

where $L_G V(x) = [L_{g_1} V(x), \ldots, L_{g_m} V(x)]$, $u_c : \Omega_c \to \mathcal{U}$ is a state feedback control law, and α is a class $\mathcal{K}$ function.

Remark 3.1. Note that the requirement for V in Assumption 3.2 is different from that of a control Lyapunov function (CLF) defined for systems without input constraints, which essentially requires the negative definiteness of $\dot{V}$ over the entire state space. Specifically, this assumption requires the negative definiteness of $\dot{V}$ only over a finite region in the state space, turning it into a constrained CLF (see also [103]). While the size of this region varies on a case-by-case basis (the nonlinear system and the choice of the Lyapunov function), a local CLF (computed based on linearization) can be always used to ascertain (and verify) this assumption over some neighborhood of the origin.

We now present an assumption for the design of high-gain observers.

Assumption 3.3. [96] There exist integers ω_i, $i = 1, \ldots, p$, with $\sum_{i=1}^{p} \omega_i = n$, and a coordinate transformation $\zeta = T(x, u)$ such that if $u = \bar{u}$, where $\bar{u} \in \mathcal{U}$ is a constant vector, then the representation of the system of Eq. (3.1) in the ζ coordinate takes the following form:

$$\begin{aligned} \dot{\zeta} &= A\zeta + B\varphi(x, \bar{u}) \\ y &= C\zeta \end{aligned} \tag{3.3}$$

where $\zeta = [\zeta_1, \ldots, \zeta_p]^{\mathrm{T}} \in \mathbb{R}^n$, $A = \text{blockdiag}[A_1, \ldots, A_p]$, $B = \text{blockdiag}[B_1, \ldots, B_p]$, $C = \text{blockdiag}[C_1, \ldots, C_p]$, $\varphi = [\varphi_1, \ldots, \varphi_p]^{\mathrm{T}}$, $\zeta_i = [\zeta_{i,1}, \ldots, \zeta_{i,\omega_i}]^{\mathrm{T}}$, $A_i = \begin{bmatrix} 0 & I_{\omega_i - 1} \\ 0 & 0 \end{bmatrix}$,

with I_{ω_i-1} being a $(\omega_i-1)\times(\omega_i-1)$ identity matrix, $B_i=[0^{\mathrm{T}}_{\omega_i-1},1]^{\mathrm{T}}$, with 0_{ω_i-1} being a vector of zeros of dimension ω_i-1, $C_i=[1,0^{\mathrm{T}}_{\omega_i-1}]$, and $\varphi_i(x,\bar{u})=\varphi_{i,\omega_i}(x,\bar{u})$, with $\varphi_{i,\omega_i}(x,\bar{u})$ defined through the successive differentiation of $h_i(x)$: $\varphi_{i,1}(x,\bar{u})=h_i(x)$ and $\varphi_{i,j}(x,\bar{u})=\frac{\partial\varphi_{i,j-1}}{\partial x}[f(x)+G(x)\bar{u}], j=2,\dots,\omega_i$. Furthermore, the functions $T:\mathbb{R}^n\times\mathcal{U}\to\mathbb{R}^n$ and $T^{-1}:\mathbb{R}^n\times\mathcal{U}\to\mathbb{R}^n$ are $\mathcal{C}^1$ functions on their domains of definition.

We next present a design of high-gain observers for output feedback control, where the input is prescribed at discrete times $t_k=k\Delta, k=0,\dots,\infty$, with Δ being the hold-time of the control action. For $t\in[t_k,t_{k+1})$, an output feedback controller using high-gain observers is formulated as follows:

$$\dot{\hat{\zeta}}=A\hat{\zeta}+B\varphi_0(\hat{x},u(t_k))+H(y-C\hat{\zeta}) \tag{3.4a}$$

$$\hat{\zeta}(t_k)=T(\hat{x}(t_k),u(t_k)) \tag{3.4b}$$

$$u=u_c(\mathrm{sat}(\hat{x}(t_k)))\text{ for all }t\in[t_k,t_{k+1}) \tag{3.4c}$$

where $\hat{x}$ and $\hat{\zeta}$ denote the estimates of x and ζ, respectively, $H=\mathrm{blockdiag}[H_1,\dots,H_p]$ is the observer gain, $H_i=\left[\frac{a_{i,1}}{\varepsilon},\dots,\frac{a_{i,\omega_i}}{\varepsilon^{\omega_i}}\right]^{\mathrm{T}}$, with $s^{\omega_i}+a_{i,1}s^{\omega_i-1}+\cdots+a_{i,\omega_i}=0$ being a Hurwitz polynomial and ε being a positive constant to be specified, and $\hat{x}(t_k)=T^{-1}(\hat{\zeta}(t_k^-),u(t_{k-1}))$ for $k=1,\dots,\infty$. The initial state of the observer is denoted by $\hat{x}_0:=\hat{x}(0)$, which takes values from any compact set $\mathcal{Q}\subseteq\mathbb{R}^n$. In the transformed coordinate, the state estimate in the ζ coordinate is re-initialized at discrete times to account for the possible changes in the input. A saturation function is used to scale back the estimate (passed to the controller) to lie within the state feedback stability region (to prevent the peaking phenomenon and enable using the state feedback control law designed for the same region), which is defined as follows:

$$\mathrm{sat}(\hat{x})=\begin{cases}\hat{x}, & \text{for }\hat{x}\in\Omega_c\\ \beta\hat{x}, & \text{for }\hat{x}\notin\Omega_c\end{cases} \tag{3.5}$$

where $\beta\in(0,1)$ is a scaling factor such that $V(\beta\hat{x})=c$ and the computation of β is specific to the choice of the Lyapunov function. For a quadratic CLF, it may be computed as $\beta=\sqrt{\frac{c}{V(\hat{x})}}$.

The subsequent analysis (see Proposition 3.1) requires the global boundedness of φ_0 formalized in Assumption 3.4 below (note that the particular choice of φ_0 only affects the observer performance; it can always be chosen as zero to satisfy this assumption).

Assumption 3.4. $\varphi_0(x,u)$ is a $\mathcal{C}^0$ function on its domain of definition and globally

bounded in x.

Remark 3.2. Note that the high-gain observer of Eqs. (3.4a) and (3.4b) generalizes (along similar lines as [96]) the class of nonlinear systems to which this type of observers can be applied in comparison to the results on the standard high-gain observer design (see, e.g., [75, 92–95, 104, 105]). The observer design exploits the fact that the control input is determined at discrete times and kept constant until the next computation (see Eq. (3.4c)). In most existing results on high-gain observer designs, the input information is either not available due to the presence of a continuous-time controller [92, 93, 105] or not used in the observer design in the presence of a discrete-time controller [75, 94, 95, 104]. In other words, the standard high-gain observer is developed for systems under a coordinate transformation $\zeta = T(x)$, which is a special case of $\zeta = T(x,u)$. While a similar design has been studied in [96], it assumes the locally Lipschitz continuity of the control input in the system state. This assumption is in general hard to verify particularly for MPC implementations. Because the control input is obtained by solving a nonlinear dynamic optimization problem, an explicit expression of the control law is generally not available. As stated earlier, the satisfaction of the alternate assumption used in this chapter, can be readily verified (i.e., whether or not a particular choice of the constrained CLF yields a meaningful stability region).

Let $D = \text{blockdiag}[D_1, \ldots, D_p]$, where $D_i = \text{diag}[\varepsilon^{\omega_i - 1}, \ldots, 1]$, and define the scaled estimation error $e = D^{-1}(\zeta - \hat{\zeta}) \in \mathbb{R}^n$. For $t \in [t_k, t_{k+1})$, the scaled estimation error evolves as follows:

$$\begin{aligned} \varepsilon \dot{e} &= A_0 e + \varepsilon B[\varphi(x, u(t_k)) - \varphi_0(\hat{x}, u(t_k))] \\ e(t_k) &= D^{-1}[T(x(t_k), u(t_k)) - T(\hat{x}(t_k), u(t_k))] \end{aligned} \tag{3.6}$$

where $A_0 = \text{blockdiag}[A_{0,1}, \ldots, A_{0,p}]$, $A_{0,i} = [a_i, b_i]$, $a_i = [-a_{i,1}, \ldots, -a_{i,\omega_i}]^{\mathrm{T}}$, and $b_i = [I_{\omega_i - 1}, 0_{\omega_i - 1}]^{\mathrm{T}}$.

Applying the change of time variable $\tau = \dfrac{t}{\varepsilon}$ and setting $\varepsilon = 0$, the boundary-layer system is given by

$$\frac{de}{d\tau} = A_0 e \tag{3.7}$$

For the boundary-layer system, we define a Lyapunov function $W(e) = e^{\mathrm{T}} P_0 e$, where P_0 is the symmetric positive definite solution of the Lyapunov equation $A_0^{\mathrm{T}} P_0 + P_0 A_0 = -I$. Let $\lambda_{\min}$ and $\lambda_{\max}$ denote the minimum and maximum eigenvalues of P_0, respectively. Preparatory to the presentation of the main results, we first give the following proposition, which is similar to a result obtained in [92], and hence stated without proof.

Proposition 3.1. Consider the system of Eq. (3.1), for which Assumptions 3.1, 3.3, and 3.4 hold. If $x_0 := x(0) \in \Omega_b$, where $0 < b < c$, then given $b' \in (b, c)$, there exists a finite time t_e, independent of ε, such that $x(t) \in \Omega_{b'}$ for all $t \in [0, t_e]$. Furthermore, there exists $\sigma > 0$, independent of ε, such that for any $e(t) \in \mathcal{W}_o := \{e \in \mathbb{R}^n : W(e) \geq \sigma\varepsilon^2\}$ and $x(t) \in \Omega_c$, $\dot{W} \leq -\frac{1}{2\varepsilon}\|e\|^2$.

3.3 Practical Stability of the Closed-Loop System under Output Feedback Control

Consider the system of Eq. (3.1), for which Assumptions 3.1, 3.2, 3.3, and 3.4 hold, under the output feedback controller of Eq. (3.4). The stability property of the closed-loop system is formalized in Theorem 3.1 below.

Theorem 3.1. *Given any $0 < b < c$ and $d > 0$, there exist $\Delta^* > 0$ and $\varepsilon^* > 0$ such that if $\Delta \in (0, \Delta^*]$, $\varepsilon \in (0, \varepsilon^*]$, and $x_0 \in \Omega_b$, then $x(t) \in \Omega_c \; \forall \, t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$.*

Proof of Theorem 3.1. The proof is divided into two parts (see also Fig. 3.1). In the first part, we show that given $e_b > 0$, which is to be determined in the second part, there exists $\varepsilon^* > 0$ such that if $\varepsilon \in (0, \varepsilon^*]$ and $\Delta \in (0, t_e]$, then the scaled estimation error $e(t_k^-)$ enters $\mathcal{E} := \{e \in \mathbb{R}^n : \|e\| \leq e_b\}$ no later than the time t_e, which is defined in Proposition 3.1, and stays in $\mathcal{E}$ thereafter as long as $x(t)$ remains in Ω_c. In the second part, we show that for any $d > 0$, there exist $e_b^* > 0$ and $\Delta^* > 0$ such that if $e(t_k^-) \in \mathcal{E}$ for some $t_{k'} \leq t_e$, $e_b \in (0, e_b^*]$, and $\Delta \in (0, \Delta^*]$, then practical stability of the closed-loop system can be established.

Consider $\Delta \in (0, \Delta_1]$ and $\varepsilon \in (0, \varepsilon_1]$, where $\Delta_1 = t_e$ and $\varepsilon_1 = \sqrt{\frac{\gamma}{\sigma}}$, with $0 < \gamma < \min_{\|e\|=e_b} W(e)$. In order to show that $e(t_k^-)$ converges to $\mathcal{E}$, we only need to show that it converges to $\mathcal{W}_i := \{e \in \mathbb{R}^n : W(e) \leq \sigma\varepsilon^2\}$.

Part 1: We first show that $e(t_k^-)$ reaches $\mathcal{W}_i$ no later than the time t_e. Let N be the largest integer such that $N\Delta \leq t_e$. It follows from Proposition 3.1 that if $t_{k+1} \leq t_e$, $k = 0, \ldots, N-1$, then for any $e \in \mathcal{W}_o$ and $t \in [t_k, t_{k+1})$, we have

$$\dot{W} \leq -\frac{1}{2\lambda_{\max}\varepsilon} W \tag{3.8}$$

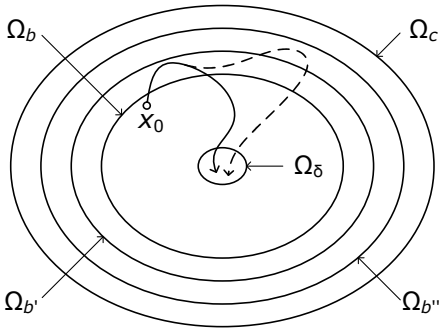

Figure 3.1: Schematic of the stability region and the evolution of the closed-loop state trajectories under fault-free (solid line) and faulty (dashed line) conditions. The notation Ω_c denotes the stability region obtained under state feedback control. For any initial condition x_0 within Ω_b, the state estimate is guaranteed to converge before the system state goes outside $\Omega_{b'}$. Subsequently, if a fault is detected and isolated before the system state goes outside $\Omega_{b''}$ (i.e., within the FDI time window), the use of the state estimate generated using measurements from the remaining healthy sensors guarantees practical stability of the closed-loop system (i.e., the system state converges to a closed ball of radius d around the origin, which contains the set Ω_δ).

It follows that

$$W(e(t_{k+1}^-)) \leq e^{-\frac{\Delta}{2\lambda_{\max}\varepsilon}} W(e(t_k)) \tag{3.9}$$

Let $\omega_{\max} = \max_{i=1,\ldots,p}\{\omega_i\}$. Since $T(x,u)$ and $T^{-1}(\zeta,u)$ are locally Lipschitz in x and ζ, respectively, and

$$e(t_k) = D^{-1}[\zeta(t_k) - \hat{\zeta}(t_k)] = D^{-1}[T(x(t_k),u(t_k)) - T(\hat{x}(t_k),u(t_k))] \tag{3.10}$$

there exists $L_1, L_2 > 0$ such that the following equation holds:

$$\begin{aligned}
\|e(t_k)\| &\leq L_1 \max\{1,\varepsilon^{1-\omega_{\max}}\}\|x(t_k) - \hat{x}(t_k)\| \\
&= L_1 \max\{1,\varepsilon^{1-\omega_{\max}}\} \times \|T^{-1}(\zeta(t_{k-1}),u(t_{k-1})) - T^{-1}(\hat{\zeta}(t_{k-1}),u(t_{k-1}))\| \\
&\leq L_1 L_2 \max\{1,\varepsilon^{1-\omega_{\max}}\} \times \max\{1,\varepsilon^{\omega_{\max}-1}\}\|e(t_k^-)\| \\
&= L_1 L_2 \eta_1(\varepsilon)\|e(t_k^-)\|
\end{aligned} \tag{3.11}$$

where $\eta_1(\varepsilon) = \varepsilon^{(\omega_{\max}-1)\mathrm{sgn}(\varepsilon-1)}$. Let $\tilde{L}_1 = L_1 L_2$. It follows from Eqs. (3.9) and (3.11) that if $e(t) \in \mathcal{W}_o$ for all $t \in [t_k, t_{k+1})$, then the following equation holds:

$$\begin{aligned}
W(e(t_{k+1})) &\leq \lambda_{\max}\|e(t_{k+1})\|^2 \\
&\leq \lambda_{\max}\tilde{L}_1^2[\eta_1(\varepsilon)]^2\|e(t_{k+1}^-)\|^2 \\
&\leq \frac{\lambda_{\max}}{\lambda_{\min}}\tilde{L}_1^2[\eta_1(\varepsilon)]^2 e^{-\frac{\Delta}{2\lambda_{\max}\varepsilon}} W(e(t_k))
\end{aligned} \tag{3.12}$$

Note that once $e(t)$ reaches $\mathcal{W}_1$, it stays there at least until the end of the same time interval. Since $T(x,u)$ is continuous, for any $x_0 \in \Omega_b$ and $\hat{x}_0 \in \mathcal{Q}$, there exists $K_1 > 0$ such that

$$\|e(0)\| \leq K_1 \eta_2(\varepsilon) \tag{3.13}$$

where $\eta_2(\varepsilon) = \max\{1, \varepsilon^{1-\omega_{\max}}\}$. To guarantee that $e(t_k^-)$ reaches $\mathcal{W}_i$ by the time t_N, it is required that the following equation hold:

$$\frac{\lambda_{\max}}{\lambda_{\min}} \tilde{L}_1^2 [\eta_1(\varepsilon)]^2 e^{-\frac{\Delta}{2\lambda_{\max}\varepsilon}} \leq \left\{ \frac{\sigma\varepsilon^2}{\lambda_{\max} K_1^2 [\eta_2(\varepsilon)]^2} \right\}^{\frac{1}{N}} \tag{3.14}$$

Rearranging the above equation gives

$$\frac{[\eta_1(\varepsilon)]^{2N}[\eta_2(\varepsilon)]^2}{\varepsilon^2} e^{-\frac{N\Delta}{2\lambda_{\max}\varepsilon}} \leq \frac{\sigma}{\lambda_{\max} K_1^2} \left(\frac{\lambda_{\min}}{\lambda_{\max}\tilde{L}_1^2} \right)^N \tag{3.15}$$

Since the left-hand side of the above inequality is continuous in ε and tends to zero as ε tends to 0, there exists $\varepsilon_2 > 0$ such that if $\varepsilon \in (0, \varepsilon_2]$, then Eq. (3.14) holds.

We then show that after the scaled estimate error $e(t_k^-)$ reaches $\mathcal{W}_i$, it stays there as long as $x(t)$ stays in Ω_c. Note that given $e(t_k^-) \in \mathcal{W}_i$, it is possible that $e(t_k)$ goes outside $\mathcal{W}_i$ due to the re-initialization to the system state and its estimate in the ζ coordinate. It follows from Eq. (3.11) that if $e(t_k^-) \in \mathcal{W}_i$, then $\|e(t_k)\| \leq \tilde{L}_1 \eta_1(\varepsilon) e_b$. To guarantee that $e(t_{k+1}^-)$ stays in $\mathcal{W}_i$, it is required that the following equation hold:

$$e^{-\frac{\Delta}{2\lambda_{\max}\varepsilon}} \leq \frac{\sigma\varepsilon^2}{\lambda_{\max}\tilde{L}_1^2 [\eta_1(\varepsilon)]^2 e_b^2} \tag{3.16}$$

It can be shown that there exists $\varepsilon_3 > 0$ such that if $\varepsilon \in (0, \varepsilon_3]$, then Eq. (3.16) holds.

In the first part of the proof, it is established that for $\varepsilon \in (0, \varepsilon^*]$, where $\varepsilon^* = \min\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$, $e(t_k^-)$ enters $\mathcal{E}$ in some finite time $t_{k'} \leq t_N \leq t_e$, where $t_{k'}$ denotes the earliest time t_k such that $e(t_k^-) \in \mathcal{E}$, and stays in $\mathcal{E}$ thereafter as long as $x(t)$ remains in Ω_c. In addition, $x(t) \in \Omega_c \, \forall \, t \in [0, t_{k'}]$.

Part 2: We first show that if the system state resides within a subset of Ω_c and the scaled estimation error is sufficiently small, then the state estimate also resides within Ω_c. It follows from the first part of the proof that we have

$$\|x - \hat{x}\| = \|T^{-1}(\zeta, u) - T^{-1}(\hat{\zeta}, u)\| \leq L_2 \eta_3(\varepsilon) \|e\| \leq L_2 \eta_3(\varepsilon_1) \|e\| \tag{3.17}$$

where $\eta_3(\varepsilon) = \max\{1, \varepsilon^{\omega_{max}-1}\}$. It can be shown that given $0 < \delta_1 < \delta_2$, there exists $\tilde{e} > 0$ such that if $e_b \in (0, \tilde{e}]$, then $V(x) \leq \delta_1$ implies $V(\hat{x}) \leq \delta_2$. It follows from Proposition 3.1 that given $b' \in (b, c)$, we have that $x(t_{k'}) \in \Omega_{b'}$. Therefore, there exists $e_{b,1} > 0$ such that if $e_b \in (0, e_{b,1}]$, then $\hat{x}(t_{k'}) \in \Omega_c$.

We then show the existence of $e_b^* > 0$ and $\Delta^* > 0$ such that if $e_b \in (0, e_b^*]$ and $\Delta \in (0, \Delta^*]$, then any state trajectory originating in $\Omega_{b'}$ at time $t_{k'}$ converges to a closed ball of radius d around the origin. Since $V(x)$ is a continuous function of the state, one can find a positive real number $\delta < b'$ such that $V(x) \leq \delta$ implies $\|x\| \leq d$. Let $\hat{\delta}$ be a positive real number such that $0 < \hat{\delta} < \delta$. If $e_b \in (0, e_{b,1}]$, the state estimate at time $t_{k'}$ can either be such that $\hat{\delta} < V(\hat{x}(t_{k'})) \leq c$ or $V(\hat{x}(t_{k'})) \leq \hat{\delta}$.

Case 1: Consider $\hat{x}(t_k) \in \Omega_c \backslash \Omega_{\hat{\delta}}$. Let $V_d(x, u) = L_f V(x) + L_G V(x) u$. For this case, we have $V_d(\hat{x}(t_k), u(t_k)) \leq -\alpha(V(\hat{x}(t_k))) < -\alpha(\hat{\delta})$. It follows from the continuity properties of $f(\cdot)$, $G(\cdot)$, and $V(\cdot)$ that $L_f V(\cdot)$ and $L_G V(\cdot)$ are locally Lipschitz on the domain of interest. Therefore, there exists $L_3 > 0$ such that

$$\begin{aligned} &|V_d(x(t_k), u(t_k)) - V_d(\hat{x}(t_k), u(t_k))| \\ &\leq L_3 \|x(t_k) - \hat{x}(t_k)\| \leq L_2 L_3 \eta_3(\varepsilon_1) \|e(t_k^-)\| \end{aligned} \tag{3.18}$$

Since the functions $f(\cdot)$ and $G(\cdot)$ are continuous, u is bounded, and $\Omega_{b'}$ is bounded, one can find $K_2 > 0$ such that $\|x(t) - x(t_k)\| \leq K_2 \Delta$ for any $\Delta \in (0, \Delta_1]$, $x(t_k) \in \Omega_{b'}$ and $t \in [t_k, t_k + \Delta)$. It follows that $\forall\, t \in [t_k, t_k + \Delta)$, the following equation holds:

$$\begin{aligned} \dot{V}(x(t)) &= V_d(\hat{x}(t_k), u(t_k)) + [V_d(x(t), u(t_k)) - V_d(x(t_k), u(t_k))] \\ &\quad + [V_d(x(t_k), u(t_k)) - V_d(\hat{x}(t_k), u(t_k))] \\ &< -\alpha(\hat{\delta}) + L_3 K_2 \Delta + L_2 L_3 \eta_3(\varepsilon_1) \|e(t_k^-)\| \end{aligned} \tag{3.19}$$

Consider $\Delta \in (0, \Delta_2]$, where $\Delta_2 = \frac{\alpha(\hat{\delta})}{3 L_3 K_2}$, and $e_b \in (0, e_{b,2}]$, where $e_{b,2} = \frac{\alpha(\hat{\delta})}{3 L_2 L_3 \eta_3(\varepsilon_1)}$. Then, we have

$$\dot{V}(x(t)) < -\frac{1}{3}\alpha(\hat{\delta}) < 0 \tag{3.20}$$

Since $\dot{V}(x(t))$ remains negative over $[t_k, t_k + \Delta)$, $x(t)$ remains in Ω_c over the same time interval, and $V(x(t_k + \Delta)) < V(x(t_k))$.

If $\hat{x}(t_{k'}) \in \Omega_c \backslash \Omega_{\hat{\delta}}$, we have $\dot{V}(x(t)) < 0$ over $[t_{k'}, t_{k'} + \Delta)$. It follows that $\hat{x}(t_{k'+1}) \in \Omega_c$ for $e_b \in (0, e_{b,1}]$. Similarly, it can be shown that for $t_k > t_{k'}$, $\dot{V}(x(t))$ remains negative until $\hat{x}(t_k)$ reaches $\Omega_{\hat{\delta}}$.

Case 2: Consider $\hat{x}(t_k) \in \Omega_{\hat{\delta}}$. Let δ' be a positive real number such that $\hat{\delta} < \delta' < \delta$. There exists $e_{b,3} > 0$ such that if $e_b \in (0, e_{b,3}]$, then $V(\hat{x}) \leq \hat{\delta}$ implies $V(x) \leq \delta'$. $\{x \in \mathbb{R}^n : \|x - \hat{x}\| \leq L_2 \eta_3(\varepsilon_1) e_{b,3} \, \forall \, \hat{x} \in \Omega_{\hat{\delta}}\} \subset \Omega_\delta$. Since $V(x)$ is continuous, and x evolves continuously in time, there exists $\Delta_3 > 0$ such that for $x(t_k) \in \Omega_{\delta'}$, if $\Delta \in (0, \Delta_3]$, then $V(x(t)) \leq \delta$ for any $t \in [t_k, t_k + \Delta)$. If $\Delta \in (0, \Delta_3]$, we have $x(t_{k+1}) \in \Omega_\delta$. It follows that $\hat{x}(t_{k+1}) \in \Omega_c$ for $e_b \in (0, e_{b,1}]$.

For $e_b \in (0, e_b^*]$ and $\Delta \in (0, \Delta^*]$, where $e_b^* = \min\{e_{b,1}, e_{b,2}, e_{b,3}\}$ and $\Delta^* = \min\{\Delta_1, \Delta_2, \Delta_3\}$, it can be shown by iteration that any state trajectory originating in $\Omega_{b'}$ at time $t_{k'}$ converges to the set Ω_δ, and hence converges to the closed ball of radius d around the origin.

In the second part of the proof, it is established that for any $d > 0$ there exists $e_b^* > 0$ and $\Delta^* > 0$ such that if $e(t_{k'}^-) \in \mathcal{E}$, $e_b \in (0, e_b^*]$, and $\Delta \in (0, \Delta^*]$, then $x(t) \in \Omega_c \, \forall \, t \geq t_{k'}$ and $\limsup_{t \to \infty} \|x(t)\| \leq d$.

In summary, it is shown that given any $0 < b < c$ and $d > 0$, there exist $\Delta^* > 0$ and $\varepsilon^* > 0$ such that if $\Delta \in (0, \Delta^*]$, $\varepsilon \in (0, \varepsilon^*]$, and $x_0 \in \Omega_b$, then $x(t) \in \Omega_c \, \forall \, t \geq 0$ and $\limsup_{t \to \infty} \|x\| \leq d$. This concludes the proof of Theorem 3.1. □

Remark 3.3. Note that the locally Lipschitz continuity of the coordinate transformation functions is used to build the relationship between the values of the state estimate in the transformed coordinate for different values of the input to account for the changes at discrete times (see Eq. (3.11)). Exploiting this relationship (not used in the standard high-gain observer design), it is shown that although the scaled estimation error may deviate from the origin due to the changes in the input, a sufficiently small ε can make it be at an inner level surface at the next update time until the scaled estimation error $e(t_k^-)$ reaches the neighborhood of the origin ($\mathcal{W}_i$), as illustrated in Fig. 3.2. Therefore, it is unnecessary to require that it converge to the neighborhood of the origin at the end of the first time interval as in [96]. In addition, it is shown in the proof that the scaled estimation error stays in the terminal set $\mathcal{E}$ ultimately. This implies that the state estimate converges sufficiently close to its true value at discrete times.

3.4 Fault Isolation and Handling Mechanism Design

In this section, we present a fault isolation logic based on the assumption that only one fault takes place (see Remark 3.9 for an extension to multiple faults); that is, if $\tilde{y}_i \neq 0$ then $\tilde{y}_j \equiv 0$

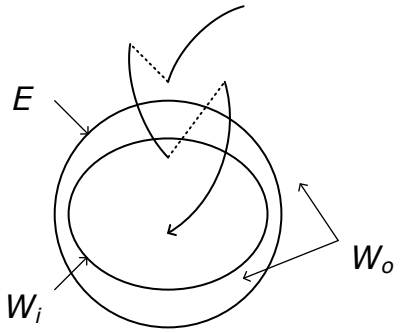

Figure 3.2: Schematic of the evolution of the scaled estimation error. $\mathcal{E}$ is the terminal set and $\mathcal{W}_i$ is the level set of the Lyapunov function contained in $\mathcal{E}$. Note that after convergence, while jumps resulting from input changes may drive the estimation error outside $\mathcal{E}$ (see the dotted lines), by the end of each interval, the estimation error is guaranteed to be within $\mathcal{E}$ (see the solid lines).

for all $j \in \{1, \ldots, p\} \backslash \{i\}$. We first design p high-gain observers for the system of Eq. (3.1) under different sensor configurations according to Section 3.3. To this end, let $y^i = h^i(x) + \tilde{y}^i \in \mathbb{R}^{p-1}$ denote the system output used in the design of the ith observer, where $y^i = [y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_p]^{\mathrm{T}}$, $h^i(x) = [h_1(x), \ldots, h_{i-1}(x), h_{i+1}(x), \ldots, h_p(x)]^{\mathrm{T}}$, and $\tilde{y}^i = [\tilde{y}_1, \ldots, \tilde{y}_{i-1}, \tilde{y}_{i+1}, \ldots, \tilde{y}_p]^{\mathrm{T}}$. The FDI design relies on the satisfaction of Assumption 3.5 stated in the following.

Assumption 3.5. For the system of Eq. (3.1), Assumptions 3.3 and 3.4 hold for the ith high-gain observer design, which uses y^i as the system output, $i = 1, \ldots, p$.

Remark 3.4. Assumption 3.5 requires that the system should be observable with any $p-1$ outputs. This results in a possibility of designing p observers, each of which uses $p-1$ measured outputs (in addition to the one that uses all p outputs for the purpose of control under fault-free conditions). Note that this requirement is more general than that of physical redundancy of sensors (where multiple sensors are used to measure the same output), and can be satisfied by sensors that measure different variables, but have analytical redundancy (in the sense of enabling full-state estimation). Note also that the relaxation on the system structure for the high-gain observer design presented in Section 3.3 aids in the ability to satisfy the above requirement, making it possible to isolate faults in any of the p sensors.

We now show a fault detection mechanism through the ith observer. The key idea is to check the error between the state estimate provided by the high-gain observer and its expected trajectory, which is computed using a state predictor and an accurate enough state estimate at a previous time. To this end, let $\hat{x}^0$ denote the state estimate generated using all the outputs (i.e., under the nominal sensor configuration), and $\hat{x}^i$ denote the one provided

by the ith observer (i.e., under the ith sensor configuration). For the same set of the outputs, let $\tilde{x}^i \in \mathbb{R}^n$ denote the state prediction, and $\tilde{x}^i(0) = \hat{x}^i(0)$. With $\hat{\tilde{x}}^i(t_{k-T}) = \hat{x}^i(t_{k-T})$ as the initial condition, the state predictor is designed as follows:

$$\dot{\hat{\tilde{x}}}^i = f(\hat{\tilde{x}}^i) + G(\hat{\tilde{x}}^i)u, t \in [t_{k-T}, t_k) \tag{3.21}$$

where $\hat{\tilde{x}}^i \in \mathbb{R}^n$ denotes the state of the model used in the predictor, and T denotes the prediction horizon: $T = 1$ if $0 < t_k \leq t_{k'}$; $T = k - k'$ if $t_{k'} < t_k \leq t_{k'+T_p}$; and $T = T_p$ if $t_k > t_{k'+T_p}$, with a positive integer T_p being the prediction horizon after the initialization period. By solving Eq. (3.21), we have $\tilde{x}^i(t_k) = \hat{\tilde{x}}^i(t_k)$. The corresponding residual (at the discrete time t_k) is defined as follows:

$$r_i(k) = \|\tilde{x}^i(t_k) - \hat{x}^i(t_k)\| \tag{3.22}$$

The proposition below presents the fault detection mechanism rigorously. To this end, let a superscript i denote the ith sensor configuration, and t_f denote the time of fault occurrence.

Proposition 3.2. Consider the system of Eq. (3.1), for which Assumptions 3.1, 3.2, 3.3, 3.4, and 3.5 hold, under the output feedback controller of Eq. (3.4). Then, given any $0 < b < c$, $d > 0$, and $\delta_{0,i} > 0$, there exist $\tilde{\Delta}^* > 0$, $\varepsilon^{*,i} > 0$, and $\delta_i > 0$ such that if $\Delta \in (0, \tilde{\Delta}^*]$, $\varepsilon \in (0, \varepsilon^*]$, $\varepsilon^i \in (0, \varepsilon^{*,i}]$, $x_0 \in \Omega_b$, $t_{k'} \leq t_{k-T_p} \leq t_f$, and $r_i(k) > \delta_i$, where ε^* is defined in Theorem 3.1, then $\tilde{y}^i(t) \neq 0$ for some $t \in [t_{k'}, t_k]$. Furthermore, for $t_k > t_{k'}$, if $r_i(k-1) \leq \delta_i$ and

$$\|M_{h,i} + M_{f,i}\| > L_1^i \eta_2^i(\varepsilon^i)(\delta_{0,i} + \delta_i) \tag{3.23}$$

where $M_{h,i} = \exp\left(\frac{\Delta}{\varepsilon^i} A_0^i\right) \bar{e} + \int_{t_{k-1}}^{t_k} \kappa(\tau) B^i(\varphi^i - \varphi_0^i) d\tau$, $M_{f,i} = -\int_{t_{k-1}}^{t_k} \kappa(\tau)[D^i]^{-1} H^i \tilde{y}^i(\tau) d\tau$, and $\kappa(\tau) = \exp\left(\frac{t_k - \tau}{\varepsilon^i} A_0^i\right)$, holds for all $\|\bar{e}\| \leq L_1^i \eta_2^i(\varepsilon_i)(\delta_{0,i} + \delta_i)$ and $\|\varphi^i - \varphi_0^i\| \leq k_i$, where $k_i > 0$ is the upper bound on $\|\varphi^i - \varphi_0^i\|$ for any $x \in \Omega_c$, then $r_i(k) > \delta_i$.

Proof of Proposition 3.2. First, we show that the system state evolves within Ω_c until time t_k. Since $V(x)$ is continuous, and x evolves continuously in time, given $b < b' < b'' < c$, there exists $\Delta_4 > 0$ such that if $x(t_k) \in \Omega_{b'}$ and $\Delta \in (0, \Delta_4]$, then $V(x(\tau)) \leq b''$ for any $\tau \in [t_k, t_k + T_p\Delta]$. It follows from the proof of Theorem 3.1 that there exist $\tilde{\Delta}^* = \min\{\Delta^*, \Delta_4\}$ such that if $t_f \geq t_{k-T}$, then $x(t) \in \Omega_{b''}$ for all $t \in [0, t_k]$ (see Fig. 3.1 for an illustration).

Next, we show that if the residual breaches the threshold, then a fault takes place. Since $f(x, u)$ is continuous and locally Lipschitz, given $\delta_{0,i} > 0$, there exists $e_b^{*,i} > 0$ such that if

$\|\tilde{x}(t_{k-T_p}) - x(t_{k-T_p})\| < L_2^i \eta_3^i(\varepsilon^i) e_b^{*,i}$, then $\|\tilde{x}(t) - x(t)\| < \delta_{0,i}$ for any $t \in [t_{k-T_p}, t_k]$ (see Theorem 3.5 in [106]). It follows from the proof of Theorem 3.1 that given $e_b^{*,i} > 0$, there exists $\varepsilon^{*,i} > 0$ such that if $\varepsilon^i \in (0, \varepsilon^{*,i}]$ and $t_{k-T} \geq t_{k'}$, then $\|e^i(t_k)\| \leq e_b^{*,i}$ for any $k \geq k'$, and consequently $\|e^i(t_{k-T})\| \leq e_b^{*,i}$. In the absence of faults, the following equation holds:

$$\begin{aligned} r_i(k) &= \|\tilde{x}^i(t_k) - \hat{x}^i(t_k)\| \\ &\leq \|\tilde{x}^i(t_k) - x^i(t_k)\| + \|x^i(t_k) - \hat{x}^i(t_k)\| \\ &\leq \delta_{0,i} + L_2^i \eta_3^i(\varepsilon^i)\|e_i(t_k)\| \\ &\leq \delta_{0,i} + L_2^i \eta_3^i(\varepsilon^i) e_b^{*,i} \end{aligned} \tag{3.24}$$

Let $\delta_i = \delta_{0,i} + L_2^i \eta_3^i(\varepsilon^i) e_b^{*,i}$. Therefore, $r_i(k) > \delta_i$ implies that $\tilde{y}^i(t) \neq 0$ for some $t \in [t_{k'}, t_k]$.

Finally, we show that if the residual does not breach the threshold at the previous time and Eq. (3.23) is satisfied, then the residual breaches the threshold at the current time. To this end, consider the scaled error dynamic system subject to sensor faults for $t \in [t_{k-1}, t_k)$ as follows:

$$\dot{e}^i = \frac{1}{\varepsilon^i} A_0^i e^i + B^i(\varphi^i - \varphi_0^i) - [D^i]^{-1} H^i \tilde{y}^i \tag{3.25}$$

The solution to the above equation gives

$$e^i(t_k) = \exp\left(\frac{\Delta}{\varepsilon^i} A_0^i\right) e^i(t_{k-1}) + \int_{t_{k-1}}^{t_k} \kappa(\tau) \times B^i(\varphi_i - \varphi_{0,i}) d\tau - \int_{t_{k-1}}^{t_k} \kappa(\tau) \times [D^i]^{-1} H^i \tilde{y}^i(\tau) d\tau \tag{3.26}$$

Then, we consider two cases: (1) $t_f \geq t_{k-1}$ and (2) $t_f < t_{k-1}$. For the first case, it follows from Eq. (3.11) that $\|e(t_{k-1})\| \leq \tilde{L}_1^i \eta_1^i(\varepsilon^i) e_b^{*,i}$. For the second case, we have $\|e(t_{k-1})\| \leq L_1^i \eta_2^i(\varepsilon^i)(\delta_{0,i} + \delta_i)$, which can be shown by a contradiction argument. Suppose $\|e(t_{k-1})\| > L_1^i \eta_2^i(\varepsilon^i)(\delta_{0,i} + \delta_i)$. Then, we have

$$\|x^i(t_{k-1}) - \hat{x}^i(t_{k-1})\| \geq \frac{1}{L_1^i \eta_2^i(\varepsilon^i)} \|e(t_{k-1})\| > \delta_{0,i} + \delta_i \tag{3.27}$$

Because $r_i(k-1) \geq \big|\|\tilde{x}^i(t_{k-1}) - x^i(t_{k-1})\| - \|x^i(t_{k-1}) - \hat{x}^i(t_{k-1})\|\big|$ and $\|\tilde{x}^i(t_{k-1}) - x^i(t_{k-1})\| \leq \delta_{0,i}$, it follows from Eq. (3.27) that we have

$$r_i(k-1) > \delta_i \tag{3.28}$$

The above equation contradicts the condition that $r_i(k-1) \leq \delta_i$, which shows that $\|e(t_{k-1})\| \leq L_1^i \eta_2^i(\varepsilon^i)(\delta_{0,i} + \delta_i)$. It can be shown that $\tilde{L}_1^i \eta_1^i(\varepsilon^i) = L_1^i \eta_2^i(\varepsilon^i) L_2^i \eta_3^i(\varepsilon^i)$.

Consequently, we have $\tilde{L}_1^i \eta_1^i(\varepsilon^i) e_b^{*,i} < L_1^i \eta_2^i(\varepsilon^i)(\delta_{0,i} + \delta_i)$. It follows from Eq. (3.23) that for both the cases, we have

$$\|x^i(t_k) - \hat{x}^i(t_k)\| \geq \frac{1}{L_1^i \eta_2^i(\varepsilon^i)} \|e(t_k)\| > \delta_{0,i} + \delta_i \tag{3.29}$$

By a similar argument, it can be shown that $r_i(k) > \delta_i$. This concludes the proof of Proposition 3.2. □

Remark 3.5. According to Proposition 3.2, a fault is detected upon the observation of a notable discrepancy between the state estimate and prediction. This in turn, relies on sufficient accuracy of the state estimate used for prediction. This property has been established in Theorem 3.1, which enables achieving a desired rate of convergence of the estimation error ($\delta_{0,i}$). Under fault-free conditions, the residual, which describes the discrepancy between the state estimate and the predicted value, is guaranteed to be below the threshold (δ_i). Therefore, the only way that the residual breaches the threshold is that the measured outputs used in this observer design are not identical to their true values, forming the basis of the fault detection mechanism. Note also that Proposition 3.2 establishes rigorous conditions on the class of faults that are detectable by the proposed method. According to these conditions, a fault is detected when its accumulated effect (possibly through multiple time intervals) is significant enough to trigger an alarm.

With the ability of detecting a fault in a subset of the sensors, we then present a method to isolate the fault and preserve practical stability of the closed-loop system. This is formalized in Theorem 3.2 below.

Theorem 3.2. *Consider the system of Eq. (3.1), for which Assumptions 3.1, 3.2, 3.3, 3.4, and 3.5 hold, under the output feedback controller of Eq. (3.4) and the fault detection design of Proposition 3.2. If $t_{k'} \leq t_{k-T_p} \leq t_f$ and $r_i(k) > \delta_i$ for all $i \in \{1, \ldots, p\} \backslash \{j\}$, then $\tilde{y}_j(t) \neq 0$ for some $t \in [t_{k'}, t_k]$. Let t_d denote the time of fault isolation. Then, given any $0 < b < c$ and $d > 0$, there exists $\tilde{\varepsilon}^{*,i} > 0$ such that if $\Delta \in (0, \tilde{\Delta}^*]$, $\varepsilon \in (0, \varepsilon^*]$, $\varepsilon^i \in (0, \tilde{\varepsilon}^{*,i}]$, $x_0 \in \Omega_b$, where $\tilde{\Delta}^*$ is defined in Proposition 3.2 and ε^* defined in Theorem 3.1, then the control law*

$$u(t) = u_c(\text{sat}(\hat{x}^{l(t_k)}(t_k))) \text{ for all } t \in [t_k, t_{k+1}) \tag{3.30}$$

and the switching rule

$$l(t) = \begin{cases} 0, & 0 \leq t < t_d \\ j, & t_d \leq t \end{cases} \tag{3.31}$$

guarantee that $x(t) \in \Omega_c$ for all $t \in [0, \infty)$ and $\limsup_{t \to \infty} \|x\| \leq d$.

Proof of Theorem 3.2. First, we show a fault taking place in the jth sensor by a contradiction argument, using the results of Proposition 3.2. Suppose that a fault takes place in some sensor indexed by $s \in \{1, \ldots, p\} \backslash \{j\}$. Since $r_s(k) > \delta_s$, a fault must have taken place in some sensor indexed by $w \in \{1, \ldots, p\} \backslash \{s\}$. Note that $w \neq s$, which is contradictory to the assumption that only one sensor fault takes place. Therefore, $r_i(k) > \delta_i$ for all $i \in \{1, \ldots, p\} \backslash \{j\}$ implies that a fault takes place in the jth sensor.

Then, we show practical stability of the closed-loop system under the control law of Eq. (3.30) and the switching rule of Eq. (3.31) with the focus on the analysis for the time interval after time t_d. It follows from the proof of Theorem 3.1 that there exists $\tilde{e}^i_{b,1} > 0$ such that if $x(t_k) \in \Omega_{b''}$ and $e^i_b \in (0, \tilde{e}^i_{b,1}]$, then $\hat{x}^i(t_k) \in \Omega_c$. Furthermore, given $\tilde{e}^{*,i}_b = \min\{\tilde{e}^i_{b,1}, e^i_{b,2}, e^i_{b,3}, e^{*,i}_b\}$, there exists $\tilde{\varepsilon}^{*,i} > 0$ such that if $\varepsilon^i \in (0, \tilde{\varepsilon}^{*,i}]$, then $e^i(t_k) \leq \tilde{e}^{*,i}_b$ for any $k \geq k'$, and consequently $e^i(t_d) \leq \tilde{e}^{*,i}_b$. It follows from the proof of Proposition 3.2 that $x(t_d) \in \Omega_{b''}$. Therefore, if $\varepsilon^i \in (0, \tilde{\varepsilon}^{*,i}]$ for all $i \in \{1, \ldots, p\}$, then $\hat{x}^j(t_d) \in \Omega_c$. The rest of the proof follows from the same line of arguments as Part 2 of the proof of Theorem 3.1, and is omitted. This concludes the proof of Theorem 3.2. □

Remark 3.6. In contrast to the existing results using a bank of Luenberger observers or Kalman filters designed for linear systems, the fault isolation mechanism in Theorem 3.2 explicitly takes system nonlinearity into account through the design of a bank of high-gain observers, with each driven by $p - 1$ outputs. Specifically, a fault is isolated when all the residuals for which the corresponding observers use measurements from the faulty sensor breach their thresholds. In contrast, the residual generated without using the erroneous measurements should be below its thresholds. Upon fault isolation, nominal operation can be continued by using the sensor configuration consisting of the remaining healthy sensors. Note also that the idea of the proposed method can be extended for systems that are observable only for certain subsets of the outputs. In that case, the faulty sensor can be "isolated" to be in the intersection of the subsets of the sensors that lead to detection alarms.

Remark 3.7. Note that the proposed FDI scheme remains applicable under any admissible control as long as the system state evolves within a compact set. The output feedback control design in Section 3.3 provides one way to guarantee that the system state evolves within a positively invariant set. Note also that Theorem 3.2 requires that faults be isolated within a certain time window. To this end, a "cushion" (see the region $\Omega_{b''} \backslash \Omega_{b'}$ in Fig. 3.1) is built to account for possible runaway behaviors between fault occurrence and declaration within the time window dictated by the prediction horizon T. In most practical situations, a sensor fault will likely cause the system state to drift (not necessarily run-

away), while keeping it within the stability region and maintaining the applicability of the proposed FDI design.

Remark 3.8. Note that the FDI scheme is presented using high-gain observers because of their ability to deal with the system nonlinearity, and provide a convergence property at a desired rate. This property is exploited for the generation of FDI residuals. The negative impact of measurement noise can be reduced in practice by filtering the noisy measurements before state estimation (see Section 3.5 for an illustration) or adopting a switched-gain approach to achieve quick convergence initially and "stable" performance later on (see, e.g., [107]). The FDI design, however, is not restricted to this particular choice of observers; any other observer that is able to provide good convergence properties and is able to handle measurement noise better can be used instead in the proposed FDI scheme.

The design and implementation of the proposed FDI and fault-handling method of Theorem 3.2 proceed as follows (see also Fig. 3.3):

1) Given the system model of Eq. (3.1), design a state feedback control law, u_c, that satisfies Assumption 3.2 and compute the stability region estimate, Ω_c, at each point of which the derivative of the Lyapunov function, $V(x)$, can be made negative and sufficiently small by using the available input (i.e., Eq. (3.2) is satisfied).

2) Given two subsets of the stability region obtained under state feedback control, Ω_b and $\Omega_{b'}$, with $0 < b < b' < c$, compute the time t_e, by the end of which the system state remains within $\Omega_{b'}$ for any initial condition within Ω_b.

3) Given $b < b'$, and the size of the closed ball, d, to which the system state is required to converge, compute Δ^* for the system under fault-free conditions, with $\Delta^* \in (0, t_e]$, and ε^* for the high-gain observer design according to Theorem 3.1.

4) Given $b' < b'' < c$ and the prediction horizon T', compute $\tilde{\Delta}^*$ according to Proposition 3.2, and use it for the purpose of closed-loop implementation. Given the prediction error, $\delta_{0,i}$, and the size of the closed ball, d, and $b' < b''$, compute $\tilde{\varepsilon}^{*,i}$ for the ith high-gain observer design used for FDI, $i = 1, \ldots, p$, according to Theorem 3.2.

5) At each time instant t_k, monitor the residuals after the scaled estimation error converges (i.e., after the time $t_{k'}$) and

   a) If all the residuals are below their thresholds (i.e., $r_i(k) \leq \delta_i$ for all $i \in \{1, \ldots, p\}$), continue to use the state estimate, $\hat{x}^0$, that is provided by the

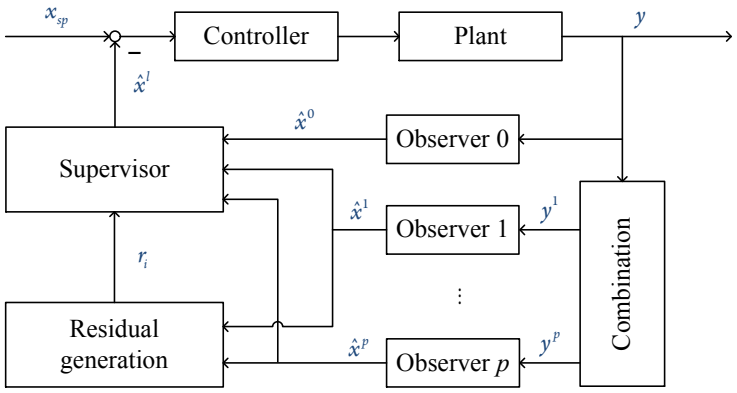

Figure 3.3: Schematic of the FDI and fault-handling framework. Before FDI, the state estimate used for feedback control is generated by observer 0, which uses all the measured outputs. After a fault takes place and FDI is achieved, the supervisor switches to the observer which uses the outputs from the remaining healthy sensors.

observer using all the outputs and compute the control input according to Eq. (3.30).

b) Otherwise, if a fault is detected and isolated (i.e., $r_i(k) > \delta_i$ for all $i \in \{1, \ldots, p\} \backslash \{j\}$), switch to use the state estimate, $\hat{x}^j$, that is provided by the observer using the outputs of the remaining healthy sensors (i.e., y^j) and compute the control input according to Eq. (3.30).

Remark 3.9. The proposed methodology can be extended to detect and isolate multiple faults. To understand this point, consider the occurrence of two faults. To detect faults, we design a bank of observers, which use combinations of $p - 1$ outputs. If all the residuals breach their thresholds, then at lease two faults have taken place. To isolate the faults, we design another bank of observers, which use combinations of $p-2$ outputs. If one residual does not breach its threshold and the remaining residuals do, then the two faults are isolated, which correspond to the outputs not used by that particular observer. Note that the above extension is based on the assumption that the system is observable with the chosen outputs so that it is possible to estimate the system state using high-gain observers.

Remark 3.10. In most existing results on model-based FDI of nonlinear process systems, actuator and sensor faults are considered separately. With the consideration of the occurrence of one (actuator or sensor) fault, however, the proposed FDI mechanism can be used to generate different patterns of residuals breaching their thresholds for an actuator fault and a sensor fault. Specifically, a sensor fault typically results in $p - 1$ residuals breaching their thresholds. If all the residuals breach their thresholds, then an actuator fault must

have taken place. This is because an actuator fault will not only result in possible errors in a state estimate, but also errors in the state prediction, which is used in the evaluation of all the residuals. A detailed analysis of the problem of fault isolation in this case is outside the scope of this chapter (see Section 7.2 for a discussion on future work).

3.5 Application to a Chemical Reactor Example

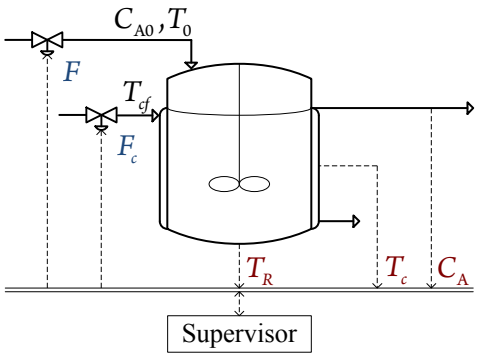

Figure 3.4: Schematic of the chemical reactor example of Section 3.5.

In this section, we consider a CSTR example, where an irreversible elementary exothermic reaction of the form $A \xrightarrow{k} B$ takes place, as shown in Fig. 3.4. The feed to the reactor consists of reactant A at a flow rate F, concentration C_{A0}, and temperature T_0. A cooling jacket is equipped to remove heat from the reactor. The cooling stream going to the jacket is at a flow rate F_c and temperature T_{cf}. The mathematical model of this chemical reactor takes the following form:

$$\begin{aligned}
\dot{C}_A &= \frac{F}{V}(C_{A0} - C_A) - k_0 e^{-E/RT_R} C_A \\
\dot{T}_R &= \frac{F}{V}(T_0 - T_R) + \frac{(-\Delta H)}{\rho c_p} k_0 e^{-E/RT_R} C_A - \frac{UA}{\rho c_p V}(T_R - T_c) \\
\dot{T}_c &= \frac{F_c}{V_c}(T_{cf} - T_c) + \frac{UA}{\rho_c c_{pc} V_c}(T_R - T_c)
\end{aligned} \tag{3.32}$$

where C_A is the concentration of species A, T_R is the temperature in the reactor, T_c is the temperature in the cooling jacket, V is the volume of the reactor, k_0, E, and ΔH are the pre-exponential constant, the activation energy, and the enthalpy of the reaction, respectively, R is the ideal gas constant, ρ and c_p are the density and the heat capacity of the fluid in the reactor, respectively, U is the overall heat transfer coefficient, A is the heat transfer area of

Table 3.1: Process parameters for the chemical reactor example of Section 3.5.

Parameter	Value	Unit
V	100	L
k_0	7.2×10^{10}	min^{-1}
E/R	8750	K
ΔH	-5×10^4	J/mol
ρ	1000	g/L
c_p	0.239	J/g·K
UA	5×10^4	J/min·K
V_c	20	L
ρ_c	1000	g/L
c_{pc}	4.2	J/g·K
C_{A0}	1	mol/L
T_0	350	K
T_{cf}	293	K

the CSTR, V_c is the volume of the cooling jacket, and ρ_c and c_{pc} are the density and the heat capacity of the cooling stream, respectively. The process parameters can be found in Table 3.1.

We first illustrate the enhanced applicability of the output feedback control design. To this end, we consider $u = [F, F_c]^{\mathrm{T}}$ and $y = [T_R, T_c]^{\mathrm{T}}$ as the input and output, respectively, where $0 \leq F \leq 60$ L/min and $0 \leq F_c \leq 10$ L/min. The control objective is to operate the process at an equilibrium point where $C_{\mathrm{A}} = 0.5$ mol/L, $T_R = 325.0$ K, and $T_c = 315.9$ K. The corresponding steady-state values of the input variables are $F = 14.6$ L/min and $F_c = 4.7$ L/min. Note that the relative degrees for the output with respect to the input are $\omega_1 = 1$ and $\omega_2 = 1$, respectively, for the process of Eq. (3.32). Therefore, the assumption of a coordinate transformation $\zeta = T(x)$ that is required for the standard high-gain observer designs (see, e.g., [75]) is not satisfied. However, it satisfies Assumption 3.3, with the following coordinate transformation: $\zeta_{1,1} = T_R$, $\zeta_{1,2} = \dot{T}_R$, and $\zeta_{2,1} = T_c$. For $t \in [t_k, t_{k+1})$, the high-gain observer is designed as follows: $\dot{\hat{\zeta}}_{1,1} = \hat{\zeta}_{1,2} + \frac{a_{1,1}}{\varepsilon}(y_1 - \hat{\zeta}_{1,1})$, $\dot{\hat{\zeta}}_{1,2} = \frac{a_{1,2}}{\varepsilon^2}(y_1 - \hat{\zeta}_{1,1})$, $\dot{\hat{\zeta}}_{2,1} = \frac{a_{2,1}}{\varepsilon}(y_2 - \hat{\zeta}_{2,1})$, and $\hat{\zeta}(t_k) = T(\hat{x}(t_k), u(t_k))$, where $\varepsilon = 0.04$, $a_{1,1} = a_{2,1} = 5$, and $a_{1,2} = 10$. A Lyapunov-based MPC design of [73] is used to illustrate the results. The hold-time for the control action is chosen as $\Delta = 0.25$ min, the prediction horizon is chosen as 2Δ, the weighting matrices used to penalize the deviations of the state and input from their nominal values are chosen as $Q_w = \text{diag}[10^5, 10^3, 10]$ and $R_w = \text{diag}[5, 50]$, respectively, and the stability region is characterized as $\{x \in \mathbb{R}^3 : V(x) = x^{\mathrm{T}} P x \leq c\}$, where x is the vector of deviation variables, $P = \begin{bmatrix} 507.90 & 9.47 & 14.02 \\ 9.47 & 0.57 & 0.53 \\ 14.02 & 0.53 & 1.05 \end{bmatrix}$,

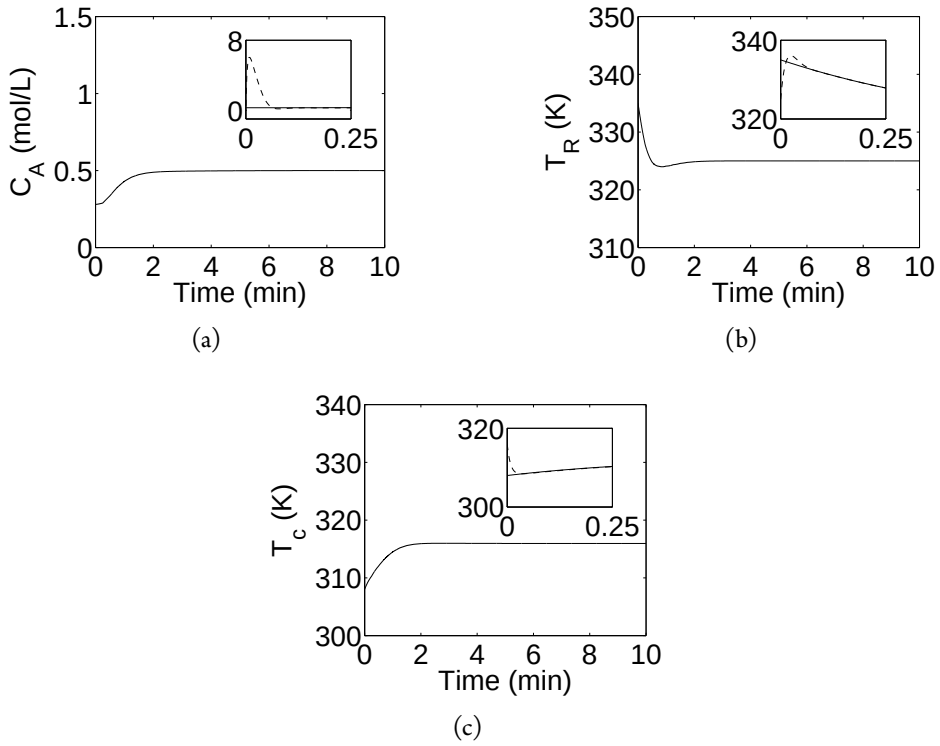

Figure 3.5: Closed-loop state (solid lines) and state estimate (dashed lines) profiles for the chemical reactor example under fault-free conditions. The insets show the quick convergence of the state estimation error.

and $c = 75.5$.

To show practical stability of the closed-loop system, consider the process from an initial condition $C_{\mathrm{A}} = 0.28$ mol/L, $T_R = 335$ K, and $T_c = 308$ K. The high-gain observer is initialized at the nominal equilibrium point. The closed-loop state profiles are shown in Fig. 3.5, where the solid and dashed lines denote the state and state estimate profiles, respectively. It is shown that the state estimates approach the process states sufficiently fast, and the controller drives the process to the nominal equilibrium point. It can be verified that the process states evolve within the stability region defined earlier. The corresponding input profiles are plotted in Fig. 3.6.

We next illustrate the FDI and fault-handling design. To this end, we first design three high-gain observers, which use outputs $y^1 = [C_{\mathrm{A}}, T_R]^{\mathrm{T}}$, $y^2 = [C_{\mathrm{A}}, T_c]^{\mathrm{T}}$, and $y^3 = [T_R, T_c]^{\mathrm{T}}$, respectively. The coordinate transformations for the first and second observers are as follows: $\zeta^1_{1,1} = C_{\mathrm{A}}$, $\zeta^1_{2,1} = T_R$, and $\zeta^1_{2,2} = \dot{T}_R$; $\zeta^2_{1,1} = C_{\mathrm{A}}$, $\zeta^2_{2,1} = T_c$, and $\zeta^2_{2,2} = \dot{T}_c$. Let T^i denote the coordinate transformation for the system with y^i being the

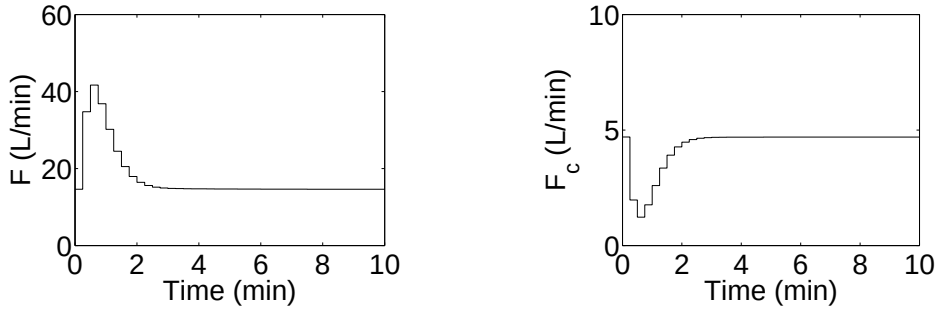

Figure 3.6: Input profiles for the chemical reactor example under fault-free conditions.

outputs, and ζ^i denote the state estimate in the corresponding transformed coordinate. The observers for the system with y^1 $(i = 1)$ and y^2 $(i = 2)$ being the outputs are designed as follows: $\dot{\hat{\zeta}}^i_{1,1} = \frac{a^i_{1,1}}{\varepsilon}(y^i_1 - \hat{\zeta}^i_{1,1})$, $\dot{\hat{\zeta}}^i_{2,1} = \hat{\zeta}^i_{2,2} + \frac{a^i_{2,1}}{\varepsilon}(y^i_2 - \hat{\zeta}^i_{2,1})$, $\dot{\hat{\zeta}}^i_{2,2} = \frac{a^i_{2,2}}{\varepsilon^2}(y^i_2 - \hat{\zeta}^i_{2,1})$, and $\hat{\zeta}^i(t_k) = T^i(\hat{x}^i(t_k), u(t_k))$, where $\varepsilon = 0.04$, $a^i_{1,1} = 5$, and $a^i_{2,1} = a^i_{2,2} = 10$. Note that the observer design with y^3 being the outputs is the same as the one used to show practical stability of the closed-loop system under fault free conditions (i.e., $\zeta^3 = \zeta$).

To show the effectiveness of the FDI and fault-handling design subject to plant-model mismatch and measurement noise, we consider a fault that takes place in C_A at time $t_f = 1.625$ min by simulating a non-abrupt bias in the concentration sensor of magnitude 0.2 mol/L, described by $\tilde{y}_1 = \left[1 - e^{-2(t-t_f)}\right] \times 0.2 \times \nu(t - t_f)$ mol/L, where $\nu(t - t_f) = \begin{cases} 0, & \text{if } t < t_f \\ 1, & \text{if } t \geq t_f \end{cases}$. Furthermore, k_0 is 2% smaller than its nominal value, and C_{A0} varies sinusoidally by a magnitude of 5% about its nominal value. The concentration and temperature measurements have combinations of eleven high-frequency (about 50 Hz) sinusoidal noises with the largest of the magnitudes being 0.01 mol/L and 0.2 K, respectively. The noisy measurements are processed through a first-order low-pass filter with the filter time constant being 0.3 sec. Full state feedback (i.e., the nominal sensor configuration) is used under fault-free conditions. In the FDI design, the prediction horizon after the initialization period is chosen as $T_p = 2$, and the thresholds are chosen as 0.025, 0.025, and 0.05 for the three FDI filters, respectively, by observing their normal variations under fault-free conditions and using a conservative upper bound to account for the presence of uncertainty and measurement noise.

The residuals, evaluated using the normalized state against its steady state value, and thresholds are shown by crosses and dashed lines, respectively, in Fig. 3.7. It can be seen

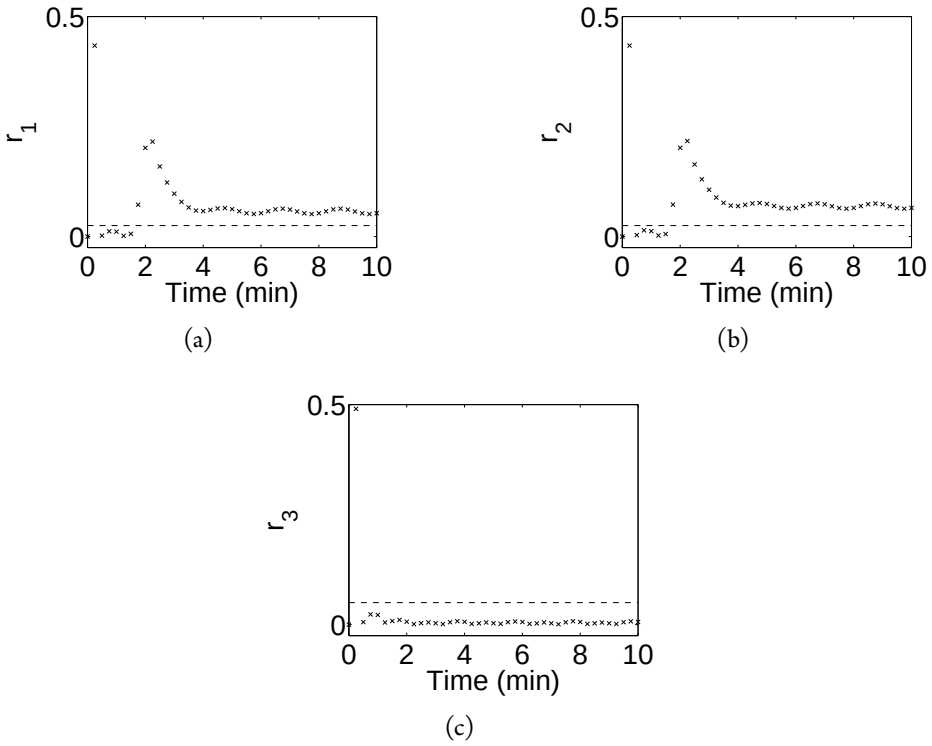

Figure 3.7: Residuals (crosses) generated using measurements of (a) C_A and T_R, (b) C_A and T_c, and (c) T_R and T_c, respectively. The fault in C_A is isolated via the residuals r_1 and r_2 breaching their thresholds (dashed lines).

that the residuals are above the thresholds at time 0.25 min (i.e., the second time instant) because of the initial transient in the observers for the state estimates to converge to their true values. After the state estimates converge, however, all the residuals are below the thresholds until the fault takes place. After the occurrence of the fault, residuals r_2 and r_3 breach their thresholds at the next time instant while r_1, which corresponds to the sensor configuration that does not use the faulty sensor, still stays below its threshold, resulting in detection and isolation of a fault in C_A at time $t_d = 1.75$ min. Upon FDI, the state estimate $\hat{x}^1$, which is generated by using measurements from the remaining healthy sensors, is used for feedback control, and practical stability of the closed-loop system is preserved, as shown by the solid (measurements) and dotted (true values) lines in Fig. 3.8. The absence of an appropriate fault-handling mechanism, however, results in degraded control performance, as shown by the dashed (measurements) and dash-dotted (true values) lines in Fig. 3.8. The corresponding input profiles are shown in Fig. 3.9 .

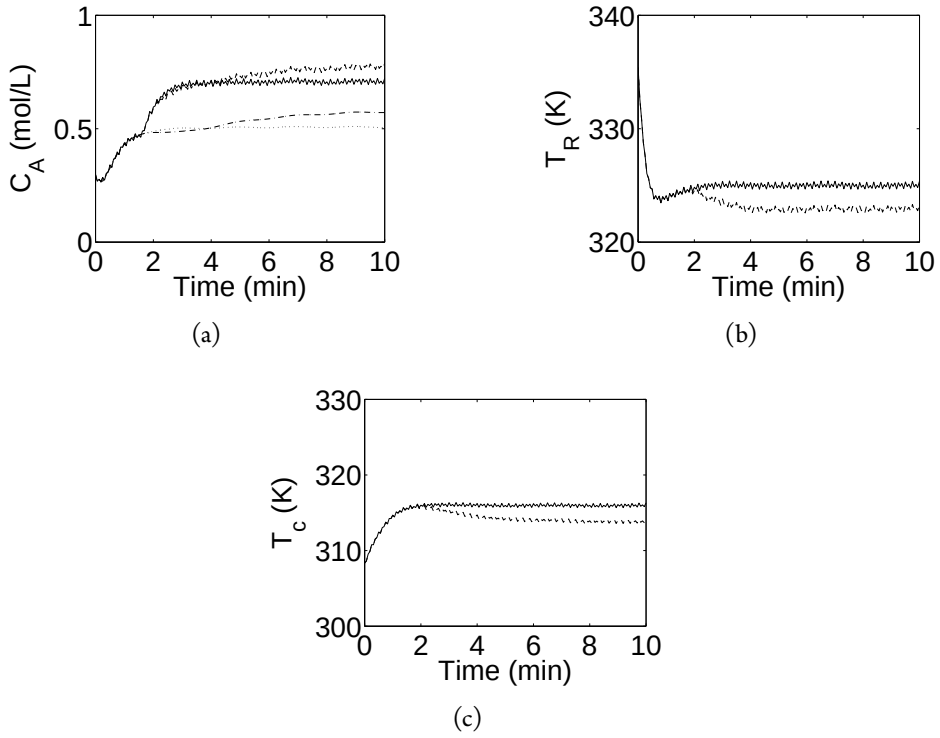

Figure 3.8: Closed-loop measurements under faulty conditions in the presence of the proposed FDI and fault-handling framework resulting in practical stability (solid lines) and in the absence of the proposed FDI and fault-handling framework resulting in degraded control performance (dashed lines). The dotted and dash-dotted lines show the evolution of the state profiles for the two cases, respectively.

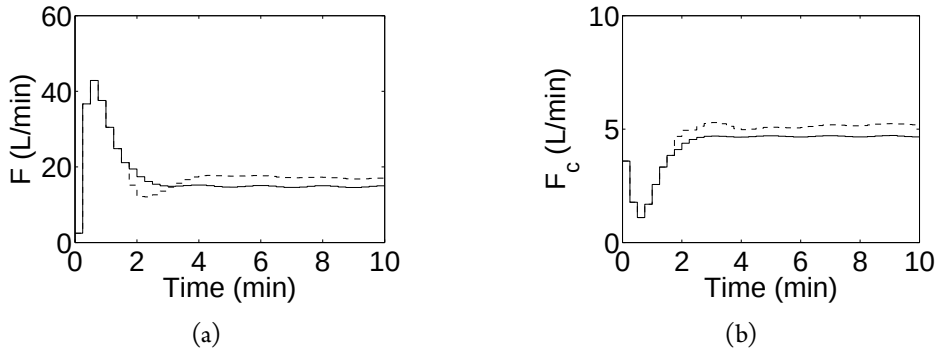

Figure 3.9: Input profiles under faulty conditions in the presence (solid lines) and absence (dashed lines) of the proposed FDI and fault-handling framework.

3.6 Conclusions

This chapter considered the problem of sensor fault isolation and FTC for nonlinear process systems subject to input constraints. The key idea of the proposed method is to exploit model-based sensor redundancy through state observer design. To this end, a high-gain observer was first presented and the stability property of the closed-loop system was rigorously established. By exploiting the enhanced applicability of the observer design, a fault isolation scheme was then proposed, which consists of a bank of observers, with each driven by a subset of the measured outputs. The residuals were defined as the discrepancies between the state estimates and their expected trajectories. A fault is isolated when all the residuals breach their thresholds except for the one that is generated without using measurements from the faulty sensor. While there are other results that use the idea of a bank of observers in the context of linear (or linear approximations of nonlinear) systems, the present results provide a rigorous detection and isolation mechanism design and analysis that explicitly handles the presence of nonlinearity and input constraints. After the fault is isolated, the state estimate generated using measurements from the healthy sensors is used in closed-loop to continue nominal operation. The implementation of the fault isolation and handling framework subject to uncertainty and measurement noise was illustrated using a chemical reactor example.

Chapter 4

Safe-Parking and Safe-Switching of Switched Nonlinear Process Systems[1]

4.1 Introduction

The previous two chapters have addressed the problem of diagnosing actuator and sensor faults, as well as handling sensor faults. The next three chapters of this thesis will consider the problem of handling severe actuator faults. As actuator faults are concerned, there have been a significant body of results on preserving nominal operation. The problem of handling faults that preclude the possibility of the continuation of nominal operation, however, has been paid attention only until recently, and has been studied using a safe-parking approach [74–77]. In these results, the key task is to design the fault-handling mechanism for a single unit or units connected in series. While a successful implement of the safe-parking design relies on a trigger resulting from FDI, these results do not explicitly consider the problem of designing FDI methods. In comparison, the results presented in the next chapters address several practical issues resulting from the complexities of chemical process systems and the integration of FDI and fault-handling mechanisms in a unified framework.

[1] The results in this chapter have been published in:

a. M. Du and P. Mhaskar. A safe-parking and safe-switching framework for fault-tolerant control of switched nonlinear systems. *Int. J. Contr.*, 84:9–23, 2011.

b. M. Du and P. Mhaskar. Uniting safe-parking and reconfiguration-based approaches for fault-tolerant control of switched nonlinear systems. In *Proceedings of the 2010 American Control Conference*, pages 2829–2834, Baltimore, MD, 2010.

In a chemical plant, the same processing equipment, such as a chemical reactor, is often used to produce multiple product types in order to meet various demands from the increasingly dynamic market. A typical example is grade transitions taking place in a polymerization process. The product quality specifications may require the use of the inlet streams carrying reactants at different conditions, such as concentrations, temperatures, or flow rates. These conditions may also change due to the complete consumption of one raw material and the switch to the use of a different one, or perturbations from other parts of a chemical plant. This gives rise to hybrid process behaviors where the continuous system dynamics are present together with the occurrence of discrete events, such as changes in raw material conditions and product specifications.

Switched systems are a subclass of hybrid systems, which operate among multiple modes with different system dynamics by following a prescribed switching schedule that describes the sequence and the times of switchings. Owing to the presence of strong nonlinearities, uncertainty, and constraints, significant research efforts have focused on the analysis and design of robust and constrained nonlinear control laws (see, e.g., [66–72, 109–112]). Research has also addressed several aspects in the analysis and controller design for hybrid systems (see, e.g., [113–117]), including results on switched systems that have addressed the problem, in the absence of faults, of determining [93] and ensuring [72, 118] that a prescribed switching schedule is implementable without loss of stability.

As with control designs, the results on handling faults in non-switched systems (i.e., nonlinear process systems without switches) are not directly applicable to switched nonlinear process systems, and there exist limited results on handling faults in the latter systems. A direct application of either the fault-tolerant or the safe-parking approaches of [27, 64, 74, 75] without accounting for the switched nature of the system would at best result in handling the fault in the first mode. However, there would be no guarantee that the closed-loop system would remain stable or the safe-parking guarantee [74, 75] would hold upon transition to the next mode of operation. Furthermore, while it may not be possible to preserve nominal operation in the currently active mode, ignoring the switched nature of the system leads to a missed opportunity of switching to a mode where nominal operation can be continued.

Motivated by the above considerations, this chapter presents a safe-parking and safe-switching framework to handle actuator faults in switched nonlinear process systems subject to input constraints. The faults considered preclude the possibility of operation at the nominal equilibrium point in the active mode. Two cases are considered according to whether or not the switching schedule can be altered during the production process. For

the case where the switching schedule is fixed, a safe-parking scheme is designed, which accounts for the switched nature, to operate the process at successive safe-park points as it transits to successive modes, which allow resumption of nominal operation after the fault is repaired. For the case where the switching schedule is adjustable, a safe-switching scheme is designed, which exploits the switched nature, to switch the process to a mode (if exists and available) where nominal operation can be preserved (through control structure reconfiguration when necessary) to continue nominal operation. The key ideas of the proposed framework are illustrated via a switched chemical reactor example, and the robustness with respect to uncertainty and measurement noise is demonstrated on an MMA polymerization process.

The rest of this chapter is organized as follows. The system description and reviews on the Lyapunov-based predictive control and the safe-parking framework for non-switched systems are presented in Section 4.2. The problem description and the assumption of a well designed nominal schedule are presented and the safe-parking and safe-switching schemes are proposed in Section 4.3. The simulation results are presented in Section 4.4. Finally, Section 4.5 presents the conclusions.

4.2 Preliminaries

This section presents the system description, followed by reviewing a Lyapunov-based predictive control design and the safe-parking approach for handling actuator faults in process systems without switches.

4.2.1 System Description

Consider a switched nonlinear system with the following state-space description:

$$\begin{aligned} \dot{x} &= f_\sigma(x) + G_\sigma(x)u \\ u &\in \mathcal{U}, \sigma \in \mathcal{K} := \{1, \ldots, p\} \end{aligned} \tag{4.1}$$

where $x \in \mathbb{R}^n$ is the vector of continuous-time state variables, $\sigma : [0, t_l] \to \mathcal{K}$ is the switching signal, which is assumed to be a piecewise continuous (from the right) function of time with t_l the total operating time, p is the number of constituent modes of the switched system, and $u \in \mathbb{R}^m$ is the vector of constrained input variables taking values in a nonempty compact convex set $\mathcal{U} := \{u \in \mathbb{R}^m : u_{\min} \leq u \leq u_{\max}\}$, where $u_{\min}, u_{\max} \in \mathbb{R}^m$ denote

the lower and upper bounds on u, respectively. The entries of $f_k(x)$ and $G_k(x)$ are assumed to be sufficiently smooth $\forall\, k \in \mathcal{K}$. The nominal switching schedule is written as follows:

$$k_1 \xrightarrow{t_1} k_2 \xrightarrow{t_2} \cdots \xrightarrow{t_{l-1}} k_l \xrightarrow{t_l} \text{end} \tag{4.2}$$

where $k_i \in \mathcal{K}\ \forall\, i \in \{1, \ldots, l\}$ with $l-1$ the number of prescribed switches, and t_i is the time when the system is switched from mode k_i to mode $k_{i+1}\ \forall\, i \in \{1, \ldots, l-1\}$. Let $x_{nom,k}$ denote the nominal equilibrium point for mode k. The control objective is to stabilize the system at the (distinct) nominal equilibrium point for each mode of operation (and not at a global equilibrium point) by following the prescribed switching schedule, which is motivated by the problem of producing multiple product grades using the same equipment in chemical processes.

Remark 4.1. In this chapter, we consider finite (total) operating time of the switched system of Eq. (4.1). This is motivated by the fact that in process industries the production scheduling usually focuses on a finite horizon in the future (e.g., due to available demands from customers). When the schedule is updated, the proposed safe-parking and safe-switching design can be revised accordingly. However, the proposed framework can be readily adapted to finite switches in a (practically) infinite operating time. In addition, we consider process systems operating between multiple nominal equilibrium points, which is motivated by grade transitions in chemical processes (each equilibrium point corresponds to a grade). From the perspective of fault-handling, the system considered in [72, 118], where a common equilibrium point is considered, is a special case of the system studied in this chapter. Also note that [72] considers the case where a pre-decided switching sequence needs to be implemented in the absence of faults, and presents an appropriate control design to achieve stabilization for the switched closed-loop system, which may be invalidated by the occurrence of faults.

4.2.2 Lyapunov-Based Predictive Control

In this section, we briefly review the stability property of the Lyapunov-based predictive control design in [73]. To this end, consider a particular mode of the switched system of Eq. (4.1) (and drop the subscripts σ and k in this section) for which a CLF $V(x)$ exists. Let Π denote the set of states where $\dot{V}(x)$ can be made negative by using the allowable values of the constrained input:

$$\Pi = \left\{ x \in \mathbb{R}^n : L_f V(x) + \inf_{u \in \mathcal{U}} L_G V(x) u \leq -\varepsilon^{**} V(x) \right\} \tag{4.3}$$

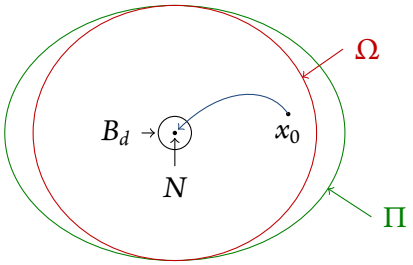

Figure 4.1: The stability property of the Lyapunov-based predictive control law. The notation N denotes the nominal operation point, and B_d denotes a ball of radius d.

where $L_G V(x) = [L_{g_1} V(x), \ldots, L_{g_m} V(x)]$ with g_i the ith column of G and ε^{**} is a positive real number. The Lyapunov-based predictive controller in [73] achieves continued decay in the value of the control Lyapunov function until it reaches a neighborhood of the equilibrium point and possesses a stability region (an estimate of which is) given by

$$\Omega = \{x \in \Pi : V(x) \leq c_{\max}\} \tag{4.4}$$

where $c_{\max}$ is a positive (preferably the largest possible) constant. The stability property of the Lyapunov-based predictive control design in [73] can be formulated as follows: given any positive real number d, there exists a positive real number ε^{**} such that if $x_0 := x(0) \in \Omega$, then $x(t) \in \Omega \; \forall \; t \geq 0$ and $\limsup_{t\to\infty} \|x(t) - x_{nom}\| \leq d$ (see Fig. 4.1). The same result holds also for initial condition within the region Π as long as the optimization problem in the predictive control formulation is successively feasible until the system state enters region Ω. Note that this control design in [73] is used only to illustrate the proposed framework in this chapter, and any other predictive controller that provides an explicit characterization of the stability region can be used instead.

4.2.3 Safe-Parking of Nonlinear Process Systems without Switches

Consider a fault scenario for one mode of the switched system of Eq. (4.1) (and drop the subscripts σ and k in this section as well), where it is assumed that the control actuator reverts to its fail-safe position upon fault occurrence. This assumption reflects the common practice to prevent the occurrence of dangerous situations due to faults, such as high temperature or high pressure, by reverting the actuator to a built-in fail-safe position. For example, a cooling valve reverts to its completely open position, and a heating valve reverts to its shut position. The vector of manipulated input variables, without loss of generality, can be decomposed into two parts: $u(t) = [u_g^{\mathrm{T}} \; u_b]^{\mathrm{T}}$, where u_g corresponds to the healthy

(good) actuators, and u_b corresponds to a failed (bad) actuator (the framework can be readily generalized to consider multiple failures). In the absence of faults, u_g takes values in $\mathcal{U}_g \subset \mathbb{R}^{m-1}$, and u_b takes values in $\mathcal{U}_b \subset \mathbb{R}$, with $\mathcal{U} = \mathcal{U}_g \times \mathcal{U}_b$, where $\mathcal{U}_g$ and $\mathcal{U}_b$ are properly defined. In the presence of the fault, u_g still takes values in $\mathcal{U}_g$, while $u_b \equiv \bar{u}_f \in \mathcal{U}_b$, where $\bar{u}_f$ denotes the fail-safe position of the control actuator (which is constant and known in advance). Essentially, the fault reduces the available control flexibility, and due to this reason the nominal equilibrium point may not be an equilibrium point in the presence of the fault (see examples in Section 4.4 for an illustration of this point).

The basic idea of the safe-parking framework for nonlinear process systems without switches is to operate the system at a temporary equilibrium point in the presence of faults and then drive the system state back to the nominal equilibrium point upon fault repair [74, 75]. The central problem of the safe-parking design is to seek an appropriate temporary equilibrium point (which is known as the safe-park point) and devise a switching rule for the controller to implement the safe-parking algorithm (i.e., to stabilize the system at the desired equilibrium points depending on the status of the fault). We characterize the set of feasible equilibrium points in the presence of the fault as follows:

$$C = \{x \in \mathbb{R}^n : f(x) + G(x) \begin{bmatrix} u_g \\ u_b \end{bmatrix} = 0, u_g \in \mathcal{U}_g, u_b \equiv \bar{u}_f \in \mathcal{U}_b\} \tag{4.5}$$

The set C is called the candidate safe-park set, and any point in C is called a safe-park point candidate (an equilibrium point subject to the failed actuator). Let Ω_{nom} and Ω_s denote the stability regions of the nominal equilibrium point and a safe-park point candidate, respectively. Similarly, we denote u_{nom} and u_s as the control inputs under the predictive control law of Section 4.2.2 to stabilize the system at the nominal equilibrium point and the safe-park point candidate, respectively. Theorem 2 below presents the safe-parking algorithm for nonlinear process systems without switches.

Theorem 4.1. [74] *Consider the constrained system of Eq. (4.1) operating in a single mode under the Lyapunov-based predictive control law of Section 4.2.2. Let t_f be the time of fault occurrence, t_d be the time of fault detection and isolation (FDI), and t_r be the time of fault repair. For $x(0) \in \Omega_{nom}$, if $x(t_d) \in \Omega_s$ and $\Omega_s \subseteq \Omega_{nom}$, then the switching rule*

$$u(t) = \begin{cases} u_{nom}(t), & 0 \leq t < t_d \\ u_s(t), & t_d \leq t < t_r \\ u_{nom}(t), & t_r \leq t \end{cases} \tag{4.6}$$

guarantees that $x(t) \in \Omega_{nom}$ $\forall\, t \in [0, t_f] \cup [t_d, \infty)$ and $\limsup_{t\to\infty} \|x(t) - x_{nom}\| \leq d$.

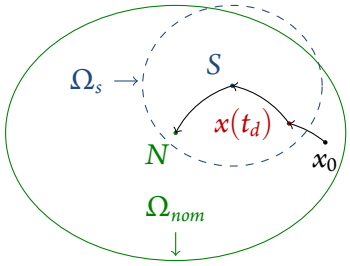

Figure 4.2: Illustration of safe-parking for an isolated unit. The notation S denotes a safe-park point. The second requirement discussed in Remark 4.2 is relaxed to only require that a neighborhood of the safe-park point reside within the stability region of the nominal equilibrium point.

Remark 4.2. Theorem 4.1 dictates that a safe-park point should be such that (1) it is an equilibrium point subject to the failed actuator and allowable values of the manipulated variables corresponding to the healthy actuators (a safe-park point candidate), (2) the system state at the time of FDI resides in its stability region, and (3) its stability region is completely contained by that of the nominal operating point. Note that the stability region of a safe-park point is characterized using reduced control action. Thus, under the switching rule of Eq. (4.6), the system can be stabilized at the safe-park point during fault repair, and nominal operation can be resumed upon fault repair (see Fig. 4.2 for an illustration). For further details on the safe-parking framework for nonlinear process systems without switches, see [74].

4.3 Handling Faults in Switched Nonlinear Process Systems

In this section, we present a safe-parking and safe-switching framework for FTC of switched nonlinear process systems subject to input constraints and actuator faults by accounting for and exploiting the switched nature of the system. In this chapter, we mainly focus on designing fault-handling schemes, which can be implemented upon FDI to take corrective control action. However, it should be noted that these designs essentially require an appropriate FDI scheme to provide timely and accurate information of faults. By imposing appropriate conditions, the proposed framework allows for determining (after the FDI system, with its possibly associated errors, declares a fault), whether or not safe operation and resumption of normal operation can be continued.

4.3.1 Problem Description

The problem considered is how to operate the switched nonlinear system of Eq. (4.1) in the presence of a fault by either accounting for the switched nature of the system to enable safe operation and to resume nominal operation the earliest it can be achieved or utilizing the presence of alternate modes to resume nominal operation. To this end, consider a scenario where a fault takes place at time t_f when the system operates in mode k_{a_0} (i.e., $\sigma(t_f) = k_{a_0}$), the fault is detected and isolated at time t_d in mode k_a (i.e., $\sigma(t_d) = k_a$), and it is repaired at time t_r in mode k_b (i.e., $\sigma(t_r) = k_b$), where $k_{a_0}, k_a, k_b \in \mathcal{K}$, with a_0, a and b the numbers indexing the sequence of operations and $1 \leq a_0 \leq a \leq b \leq l$. The fault results in the control actuator reverting to its fail-safe position upon fault occurrence. Recall that t_a and t_b denote the times when the system is switched out from modes k_a and k_b, respectively. The relation between t_f, t_d, t_a, t_r and t_b is illustrated in Fig. 4.3, where $a_0 = a$, i.e., the fault is detected and isolated while the system is in the same mode where the fault occurred (note that fault occurrence and FDI may not always take place in the same mode). In this chapter, we focus on severe faults that preclude the possibility of nominal operation in the active mode k_a. In particular, we consider the problem of fault-handling for two types of the switching schedules: a fixed schedule and a flexible schedule. For the first case, the switching sequence and switching times are fixed and cannot be changed on-line (e.g., due to a fixed availability of various streams from other units of a plant), while for the second case, the switching sequence and switching times can be adjusted, as well as the operating time in each mode (e.g., due to the availability of raw materials with various conditions). Note that if the fault is not severe (e.g., a bias that does not lead to the inability to preserve nominal operation), it can be handled via the inherent robustness of the controller design [62].

4.3.2 Assumption of a Well Designed Nominal Schedule

Before presenting the fault-handling framework, we first formalize an assumption based on the design of an appropriate switching schedule in the absence of faults. To this end, consider the switched nonlinear system described by Eq. (4.1) that operates under an appropriately designed Lyapunov-based predictive control law of Section 4.2.2 for each mode. Let Ω_{nom,k_i} denote the stability region of equilibrium point x_{nom,k_i} under nominal operation in mode k_i, with u_{nom,k_i} the nominal control input, and B_{d,nom,k_i} denote a ball of radius d (defined in Section 4.2.2) around x_{nom,k_i}. Let T^{nom}_{0,k_1} denote the maximum time it takes to reach B_{d,nom,k_1} from any $x(0) \in \Omega_{nom,k_1}$, and $T^{nom}_{k_i,k_{i+1}}$ denote the maximum time it takes to

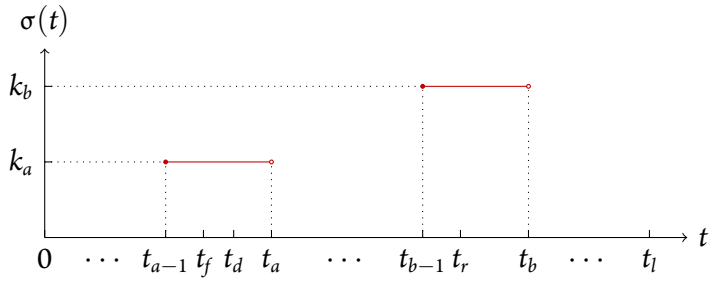

Figure 4.3: Schematic of fault occurrence, FDI, and fault repair under the nominal schedule.

reach $B_{d,nom,k_{i+1}}$ from any point within B_{d,nom,k_i}.

Assumption 4.1. For the switched nonlinear system of Eq. (4.1) subject to input constraints under the switching schedule of Eq. (4.2) and the Lyapunov-based predictive control law of Section 4.2.2 in each mode, we have that $B_{d,nom,k_i} \subseteq \Omega_{nom,k_{i+1}} \; \forall \; i \in \{1, \ldots, l-1\}$ and $T^{nom}_{k_i,k_{i+1}} \leq t_{i+1} - t_i \; \forall \; i \in \{0, \ldots, l-1\}$, where $k_0 = 0$ and $t_0 = 0$.

Remark 4.3. Assumption 4.1 merely formalizes what is expected of a well designed nominal schedule, which should have the following property: the system can be stabilized at the nominal equilibrium point in each mode as it transits to successive modes. To this end, it requires that the desired neighborhood (a ball of radius d) of the nominal equilibrium point for each mode be contained by the stability region of the nominal equilibrium point for the next mode (see Fig. 4.4). We use the desired neighborhood instead of the equilibrium point due to the discrete nature of the control implementation (the control input is implemented at the discrete instants) and finite operating time in each mode (generally the state of a dynamic system can only reach a neighborhood of the equilibrium in finite time). It also requires that the designed operating time for each mode allow the system to be stabilized at the corresponding nominal equilibrium point before the next transition. The second requirement is not conservative in practical cases, such as grade transitions in chemical processes, where a reasonable amount of product should be generated in each mode. Therefore, the time taken to stabilize should be sufficiently short compared to the operating time in a given mode.

4.3.3 Handling Faults for a Fixed Schedule

In this section, we consider the case where there is no flexibility with regard to the switching sequence and switching times. The key idea in handling faults then is upon fault occurrence

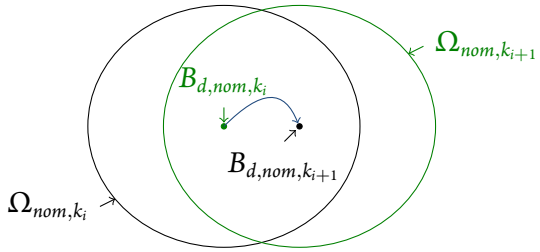

Figure 4.4: Illustration of a well designed nominal schedule.

to safe-park the system at an appropriate safe-park point for the active mode such that the system can be safe-parked in subsequent modes and to ensure that nominal operation can be resumed after the fault is repaired. To this end, let Ω_{s,k_i} denote the stability region of a safe-park point candidate (x_{s,k_i}) for mode k_i, with u_{s,k_i} the (reduced) control input of Section 4.2.2 to drive the system state to a ball of radius d around that point, which is denoted by B_{d,s,k_i}. Let T_f denote the additional time it takes to reach B_{d,s,k_a} after FDI, T_r the additional time it takes to reach B_{d,nom,k_b} after the fault is repaired, $T^s_{k_i,k_{i+1}}$ the maximum time it takes to reach $B_{d,s,k_{i+1}}$ from any point within B_{d,s,k_i}, and $T^{s,nom}_{k_i,k_{i+1}}$ the maximum time it takes to reach $B_{d,nom,k_{i+1}}$ from any point within B_{d,s,k_i} (see Remark 4.7 on the estimation of T_f and T_r). The safe-parking scheme is formalized in Theorem 4.2 below, and the proof of this theorem can be found in Appendix A.1.

Theorem 4.2. *Consider the switched nonlinear system of Eq. (4.1) subject to input constraints, for which Assumption 4.1 holds, under the Lyapunov-based predictive control law of Section 4.2.2 in each mode. Let t_f be the time of fault occurrence, t_d be the time of fault detection and isolation, and t_r be the time of fault repair. For $x(0) \in \Omega_{nom,\sigma(0)}$, if:*

1. $x(t_d) \in \Omega_{s,k_a}$ *and* $B_{d,s,k_i} \subseteq \Omega_{s,k_{i+1}}\ \forall\, i \in \{a, \ldots, l-1\}$
2. $T_f \leq t_a - t_d$ *and* $T^s_{k_i,k_{i+1}} \leq t_{i+1} - t_i\ \forall\, i \in \{a, \ldots, l-1\}$
3. $\Omega_{s,k_i} \subseteq \Omega_{nom,k_i}\ \forall\, i \in \{a, \ldots, l\}$

then the switching rule

$$u(t) = \begin{cases} u_{nom,\sigma(t)}(t), & 0 \leq t < t_d \\ u_{s,\sigma(t)}(t), & t_d \leq t < t_s \\ u_{nom,\sigma(t)}(t), & t_s \leq t \leq t_l \end{cases} \tag{4.7}$$

where $t_s = t_r$ if $T_r \leq t_b - t_r$ and $t_s = t_j$ with $j = \min\{\min\{i : T^{s,nom}_{k_i,k_{i+1}} \leq t_{i+1} - t_i, i = b, \ldots, l-1\}, l\}$ if $T_r > t_b - t_r$, guarantees that $x(t) \in \Omega_{nom,\sigma(t)}\ \forall\, t \in [0, t_f] \cup [t_d, t_l]$ and

$\|x(t_i) - x_{nom,k_i}\| \leq d \, \forall \, i \in \{1, \ldots, a_0 - 1\} \cup \mathcal{B}$, *where* $\mathcal{B} = \{b, \ldots, l\}$ *if* $T_r \leq t_b - t_r$ *and* $\mathcal{B} = \{j+1, \ldots, l\}$ *if* $T_r > t_b - t_r$.

Remark 4.4. Theorem 4.2 provides not only the switching logic for the controller but also the criteria for choosing safe-park points for the switched system of Eq. (4.1). For mode k_i ($i = a, \ldots, l$), a safe-park point candidate is termed a safe-park point if (1) the system state at the time of FDI is within its stability region (for the mode of fault occurrence) or the neighborhood of the previous safe-park point is contained by its stability region (for subsequent modes), (2) within the designed operating time for the corresponding mode, the system can be stabilized at the safe-park point candidate in the presence of the fault, and (3) its stability region is contained by that of the nominal equilibrium point. The first and second conditions ensure that the system can be stabilized at successive safe-park points as it transits to successive modes under the nominal schedule. Besides the consideration of stability regions, it also imposes a requirement on the time taken to safe-park. If this condition is not satisfied, it may happen that the state at the transition time is not close enough to the safe-park point for the mode to which it transits (i.e., outside its stability region). Then, there is no guarantee that the system can be safe-parked successively. The third condition ensures that the system state continues to evolve within the stability regions of the constituent modes at all times except the period between fault occurrence and FDI (i.e., (t_f, t_d) due to possible FDI delays), from where nominal operation can be resumed smoothly after the fault is repaired.

Remark 4.5. Most of the requirements in Theorem 4.2 can be verified, and are essentially used, in the off-line design of safe-park point candidates for the switched system under the nominal schedule. In particular, "strings" of safe-park point candidates are determined off-line (e.g., $x_{s,k_1}, \ldots, x_{s,k_l}$ is a "string" of safe-park point candidates), which satisfy the conditions in Theorem 4.2 that can be verified off-line. Then out of these candidates, an appropriate "string" is chosen on-line by considering the system state at the time of FDI. In contrast to the safe-parking framework of Theorem 4.1, it requires simultaneous design of safe-park point candidates for multiple modes, instead of designing them for each mode in isolation. Because the times of fault occurrence and fault repair are not known at the design stage, the safe-park point candidates are designed for all the modes in the nominal schedule. Note that the second requirement on the time taken to safe-park from one safe-park point candidate to the next can be readily satisfied in practice (see Remark 4.3 for more discussion).

Remark 4.6. At the time of FDI, a "string" of safe-park point candidates (e.g., $x_{s,k_a}, \ldots, x_{s,k_l}$) are chosen as safe-park points such that the system state is within the stability region of the safe-park point candidate for the mode (k_a) where the fault is detected and isolated,

and there is sufficient time to safe-park before the next transition (which can be verified by comparing the remaining operating time in mode k_a and the time taken to safe-park therein). Furthermore, out of all the safe-park point candidates satisfying the requirements in Theorem 4.2, we can choose one that minimizes a cost function penalizing the distances between the safe-park points and the nominal equilibrium points, and the control efforts during safe-parking, if an estimate of the fault repair time is available. Note that in the context of switched process systems, it might be possible to operate the system nominally (even in the presence of the fault) in some subsequent mode (if not in the currently active mode). With such a cost function in place, the safe-park point in a particular mode could actually be the nominal equilibrium point. This represents a special case of safe-parking in that mode.

Remark 4.7. Note that the time (T_f) taken to safe-park the system in the mode (k_a) where FDI takes place needs to be estimated on-line. However, the computation of T_f under the predictive controller is computationally demanding even for the nominal system. If one were to explicitly account for uncertainty, an accurate estimate of T_f would require solving a computationally expensive min-max optimization problem. One practically implementable way of estimating T_f is to run a simulation under another controller that would cause the decay of the same Lyapunov function as the predictive controller (one possibility is to use the bounded controller of [109]), under nominal conditions, and multiply the time taken under the bounded controller by a certain factor to account for robustness and the fact that the closed-loop system evolves under the predictive controller. This estimation is computationally efficient (though conservative), thereby allowing timely correction of the control action. Similarly, upon fault repair, the time (T_r) taken to stabilize in the mode (k_b) where the fault is repaired can be estimated through the same procedure as above. Also note that the proposed scheme does not require an *a priori* estimate of the fault repair time, but utilizes a "safe" zone for each safe-park point where the system can be run up until the switching time or resumption of nominal operation.

Remark 4.8. Note that for switched process systems, (in contrast to the safe-parking of non-switched process systems [74]), the time (t_s) when nominal operation is resumed is not always the same as the fault repair time (t_r). According to Theorem 4.2, if the time required to reach the nominal equilibrium point in the mode of fault repair (k_b) is less than or equal to the remaining operating time in that mode, nominal operation is resumed upon fault repair. Otherwise, the system is safe-parked in mode k_b even after the fault is repaired. In the latter case, if nominal operation were resumed in mode k_b, upon transition to the next mode there would be no guarantee that at the transition time the system state is within the corresponding stability region under nominal conditions. Due to this reason,

nominal operation is only resumed when it transits to a mode (mode $j+1$ in Theorem 4.3 if exists) where it can be done within the operating time in that mode (in most cases this would be the immediate next mode due to the reason stated in Remark 4.3). Note that it may also happen that nominal operation is not resumed even at the end of the entire operation (e.g., due to the reason that the fault is not repaired by the total operating time t_l, or there is insufficient time to stabilize at a nominal equilibrium point). In this case, $\{i : T^{s,nom}_{k_i,k_{i+1}} \leq t_{i+1} - t_i, i = b, \ldots, l-1\} = \varnothing$ (i.e., there does not exist a mode where nominal operation can be resumed), and consequently $t_s = t_j = t_l$.

Remark 4.9. Note that if a fault is detected and isolated when the next transition is imminent, a minimum-time predictive controller (one that requires to go to a target region as fast as possible) could enhance the chance of entering the desired neighborhood of the safe-park point before the next transition takes place (e.g., for the case where a conservative estimate of T_f is used). However, it still provides no *a priori* guarantee of safe-parking in mode k_a due to the constrained input and limited operating time in that mode. To deal with this extreme situation where there exist no eligible safe-park points for mode k_a due to insufficient time to safe-park, one could incorporate a terminal set constraint in the predictive controller such that the system state at the time of transition is constrained to be within the stability region of the safe-park point for the next mode. If the optimization problem in the predictive control formulation is initially and successively feasible, then at the time of transition, the system state will be within the stability region of the safe-park point for the next mode, thereby realizing successive safe-parking.

4.3.4 Handling Faults for a Flexible Schedule

In general, the presence of switched dynamics adds additional complexity that needs to be handled in the control design for fault-free systems (see, e.g., [72, 93, 118]) and the safe-parking design in Section 4.3.3. Although the safe-parking scheme can provide a guarantee for safe operation and resumption of nominal operation, it cannot essentially prevent non-nominal operation (e.g., leading to off-spec product and additional costs for further processing). The presence of additional modes of operation, however, also presents a unique possibility of handling faults in switched process systems. In this section, we consider the scenario where there is flexibility in the switching schedule, and present a safe-switching scheme which exploits the switched nature of the system (i.e., utilizing the possibility of operation in multiple modes) to continue nominal operation, thereby maximizing on-spec (although possibly off-schedule) product in chemical processes. The key idea is to seek and switch to a target mode k_c (if exists and available) where nominal operation can be contin-

ued by using the depleted control action, which is formalized in Theorem 4.3 below (the proof of this theorem can be found in Appendix A.2). To this end, let $\hat{C}_{k_c}$ denote the candidate safe-park set of Eq. (4.5) for mode k_c, $\hat{\Omega}_{k_c}$ denote the stability region of the nominal equilibrium point x_{nom,k_c} with the reduced control action, and $\hat{u}_{k_c}$ denote the corresponding control input to stabilize at x_{nom,k_c}. For the sake of simplicity, it is assumed that $\hat{\Omega}_{k_c}$ is characterized by using the same control Lyapunov function as Ω_{k_c}. Consequently, we have $\hat{\Omega}_{k_c} \subseteq \Omega_{nom,k_c}$.

Theorem 4.3. *Consider the switched nonlinear system of Eq. (4.1) subject to input constraints, for which Assumption 4.1 holds, under the Lyapunov-based predictive control law of Section 4.2.2 in each mode. Let t_f be the time of fault occurrence, t_d be the time of fault detection and isolation, and t_r be the time of fault repair. For $x(0) \in \Omega_{nom,\sigma(0)}$, if:*

1. $x(t_d) \in \Omega_{s,k_a} \subseteq \Omega_{nom,k_a}$
2. $\exists\, k_c \in \mathcal{K}$ *such that* $c > a$, $x_{nom,k_c} \in \hat{C}_{k_c}$, *and* $B_{d,s,k_a} \subseteq \hat{\Omega}_{k_c}$

then the switching rule

$$u(t) = \begin{cases} u_{nom,\sigma(t)}(t), & 0 \le t < t_d \\ u_{s,k_a}(t), & t_d \le t < t'_a \\ \hat{u}_{k_c}(t), & t'_a \le t < t'_c \\ u_{nom,\sigma'(t)}(t), & t'_c \le t \le t'_l \end{cases} \tag{4.8}$$

where t'_a is the earliest time such that $x(t) \in \hat{\Omega}_{k_c}$ after fault detection and isolation, $t'_c = \max\{t'_a + T_c, t_r, t'_a + t_c - t_{c-1}\}$ with T_c the additional time taken to reach B_{d,nom,k_c} after time t'_a, and $\sigma' : [t_d, t'_l] \to \mathcal{K}$ refers to the updated switching schedule of $k_a \xrightarrow{t'_a} k_c \xrightarrow{t'_c} k_{c+1} \xrightarrow{t'_{c+1}} \cdots \xrightarrow{t'_{l-1}} k_l \xrightarrow{t'_l}$ end with $t'_i := t'_{i-1} + t_i - t_{i-1}\ \forall\, i \in \{c+1, \ldots, l\}$, guarantees that $x(t) \in \Omega_{nom,\sigma(t)}\ \forall\, t \in [0, t_f]$, $\|x(t_i) - x_{nom,k_i}\| \le d\ \forall\, i \in \{1, \ldots, a_0 - 1\}$, $x(t) \in \Omega_{nom,\sigma'(t)}$ $\forall\, t \in [t_d, t'_l]$, and $\|x(t'_i) - x_{nom,k_i}\| \le d\ \forall\, i \in \{c, \ldots, l\}$.

Remark 4.10. The presence of multiple modes provides another option to realize FTC for switched nonlinear process systems in addition to the safe-parking scheme of Theorem 4.2. In particular, to exploit the presence of multiple modes, Theorem 4.3 requires switching the system to a mode (if exists and available) which can tolerate the failed actuator (i.e., nominal operation is achievable with the depleted control action: $x_{nom,k_c} \in \hat{C}_{k_c}$), and dictates when the switching should be made and how the remaining operation should be followed. To ensure a safe-switching, it requires a safe-park point (e.g., x_{s,k_a}) for the mode

(k_a) where the fault is detected and isolated such that its neighborhood resides in the stability region ($\hat{\Omega}_{k_c}$) of the nominal equilibrium point for the target mode (k_c) to which it is switched with the reduced control action. Upon FDI and identification of such a mode, the system is not switched to mode k_c immediately. Instead, the system state is first driven to move towards the safe-park point x_{s,k_a}, and the switching is executed when it enters the stability region $\hat{\Omega}_{k_c}$. The system operates in mode k_c at least till the system state reaches the neighborhood of the nominal equilibrium point ($t'_c \geq t'_a + T_c$) and also till the time of fault repair ($t'_c \geq t_r$), which is possible due to the flexibility of operation. Even after the fault is repaired, the system still operates in the target mode to ensure the completion of the designed operating time if it is not met at the time of fault repair ($t'_c \geq t'_a + t_c - t_{c-1}$). After the system is switched out of mode k_c, the rest of the switching schedule is followed (owing to Assumption 4.1).

Remark 4.11. In principle, Theorem 4.3 could require choosing a target mode (k_c) such that the system state at the time of FDI is within the associated stability region (if such a mode is available). In that case, immediate switching upon FDI would be allowed. However, the proposed two-stage operating policy: safe-parking in mode k_a (although without completion) and resumption of nominal operation in mode k_c, can significantly enhance the chance of resuming nominal operation in the presence of the fault with guaranteed stability (e.g., for the case where the system state at the time of FDI does not reside in the stability region of the nominal equilibrium point for any mode where nominal operation can be preserved). Note also that switching to an alternate mode could result in changes in the switching times and/or the switching sequence. In particular, if the target mode dictated by Theorem 4.3 is the next mode in the original schedule, it then essentially ends up only requiring a change in the switching time, enabling the continuation of the rest of the switching schedule. Otherwise, the switching sequence is adjusted as well by jumping over operation in modes between $k_a, \ldots, k_c$. The mode k_c is preferably the earliest eligible target mode in the remaining part of the nominal schedule to minimize skipping over modes of operation. After the revised switching sequence is completed, the supervisor could try operating the system in the missed modes (if possible) through rescheduling.

Remark 4.12. Note that the idea of control structure reconfiguration [27, 64] can also be utilized to enhance the chance of continuing nominal operation in the presence of the fault (e.g., for the case where nominal operation cannot be preserved in any mode under the active control configuration). In the reconfiguration-based approach, a set of control configurations with different choices of manipulated variables (e.g., indexed by $1, \ldots, p'$) are designed, and the stability region associated with each control configuration under nominal conditions is characterized (for each mode where nominal operation is possible under

the corresponding control configuration). The basic idea of this approach is to activate an appropriate backup control configuration to achieve nominal operation in the presence of the fault. To incorporate this approach in the proposed safe-switching scheme, Theorem 4.3 can be modified to allow choosing a target mode k_c *and* a backup control configuration j at the time of FDI that satisfy the corresponding requirements. In this case, the backup control configuration is activated at the same time as switching to mode k_c.

4.4 Simulation Examples

In this section, we first illustrate the details of the proposed framework via a switched chemical reactor example in Section 4.4.1. Then, application to a polymerization process of MMA subject to uncertainty and measurement noise is demonstrated in Section 4.4.2.

4.4.1 Illustrative Simulation Example

In this section, we illustrate the key ideas of the safe-parking and safe-switching framework via a CSTR example, where an irreversible, first-order exothermic reaction of the form A $\xrightarrow{k}$ B takes place. The process operates in three modes out of five candidates. For each mode, the inlet stream is composed of pure A with concentration $C_{A,in}$, flow rate F_σ, and temperature $T_{in,\sigma}$. The mathematical model for the process is of the following form:

$$\begin{aligned} \dot{C}_A &= \frac{F_\sigma}{V}(C_{A,in} - C_A) - k_0 e^{-E/RT_R} C_A \\ \dot{T}_R &= \frac{F_\sigma}{V}(T_{in,\sigma} - T_R) + \frac{(-\Delta H)}{\rho_m c_p} k_0 e^{-E/RT_R} C_A + \frac{Q}{\rho_m c_p V} \end{aligned} \tag{4.9}$$

where C_A is the concentration of species A in the reactor, T_R is the temperature of the reactor, Q is the rate of heat added to/removed from the reactor, k_0, E, and ΔH are the pre-exponential constant, the activation energy, and the enthalpy of the reaction, respectively, c_p and ρ_m are the heat capacity and density of the reacting mixture, respectively, and $\sigma \in \{1, 2, 2', 3, 3'\}$ is the switching signal. Under fault-free conditions, the control objective is to stabilize the reactor at the unstable equilibrium points N_1(0.80 kmol/m^3, 387.5 K), N_2(0.60 kmol/m^3, 395.0 K) and N_3(0.80 kmol/m^3, 402.5 K) in three modes (regardless of the switching schedule), respectively. In the control and fault-handing design, we consider a primary control configuration, with $C_{A,in}$ and Q as manipulated variables, and a backup control configuration, with $C_{A,in}$ and $T_{in,\sigma}$ as the manipulated variables. The inlet

Table 4.1: Process parameters for the switched chemical reactor example of Section 4.4.1.

V	0.1	m^3
R	8.314	kJ/kmol·K
k_0	72×10^9	min^{-1}
E	8.314×10^4	kJ/kmol
ΔH	-4.78×10^4	kJ/kmol
c_p	0.239	kJ/kg·K
ρ_m	1000.0	kg/m^3
F_1	0.35	m^3/min
$T_{in,1}$	315.0	K
F_2	0.30	m^3/min
$T_{in,2}$	315.0	K
F_3	0.50	m^3/min
$T_{in,3}$	335.0	K
$F_{2'}$	0.25	m^3/min
$T_{in,2'}$	325.0	K
$F_{3'}$	0.35	m^3/min
$T_{in,3'}$	300.0	K

concentration is subject to the constraint of $0 \leq C_{A,in} \leq 2.8$ kmol/m^3. The rate of heat input $Q = Q_{h1} + Q_{h2} + Q_c$, where $0 \leq Q_{h1}, Q_{h2} \leq 45$ kJ/s and -90 kJ/s $\leq Q_c \leq 0$ represent the effects of two heating streams and one cooling stream, respectively, and consequently -90 kJ/s $\leq Q \leq 90$ kJ/s. The constraint on the temperature of the inlet stream is 295 K $\leq T_{in,\sigma} \leq$ 365 K. The process parameters can be found in Table 4.1. The steady-state values of the manipulated input variables can be computed accordingly. Therefore, they are omitted for brevity.

To demonstrate the necessity to account for the switched nature of the process in the safe-parking scheme, consider a nominal schedule of $1 \xrightarrow{6\,\text{min}} 2 \xrightarrow{12\,\text{min}} 3 \xrightarrow{20\,\text{min}}$ end. In order to characterize the stability regions, we consider quadratic Lyapunov functions of the form $V(x) = x^{\mathrm{T}} P x$ (also in Section 4.4.2), where P is positive definite. The P matrices for the nominal equilibrium points of modes 1, 2, and 3 are $\left[\begin{smallmatrix} 1.2 & 0 \\ 0 & 0.0012 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 3 & 0 \\ 0 & 0.0014 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} 6.5 & 0 \\ 0 & 0.0026 \end{smallmatrix}\right]$, respectively, and the associated stability regions $\Omega_{nom,k}$ are plotted in Fig. 4.5. Consider the failure of one of the heating valves, which reverts to the shut position upon fault occurrence, leading to -90 kJ/s $\leq Q \leq 45$ kJ/s. The fault considered precludes the possibility of nominal operation under both the primary and backup control configurations in all the three modes (i.e. there exists no available value of the manipulated variables such that the nominal equilibrium point continues to be an equilibrium point in the presence of the fault). We design safe-park point candidates S_1(0.85 kmol/m^3, 405.0 K) and S_1' (1.30 kmol/m^3,

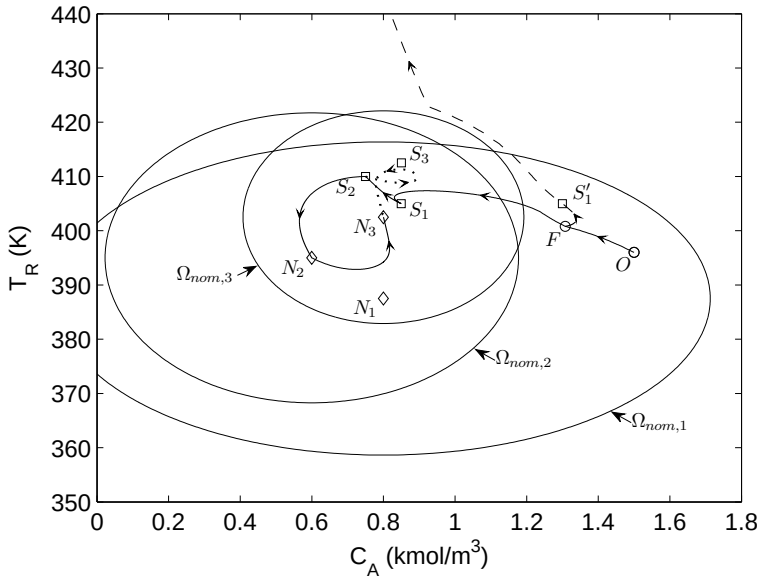

Figure 4.5: Closed-loop state trajectory for the switched chemical reactor example of Section 4.4.1 with a fixed schedule when the heating valve fails at $t_f = 0.05$ min. The dashed trajectory shows the case when the safe-park point candidate S_1' is used for mode 1 without considering the switched nature of the process and results in instability. The solid and dotted trajectories show the cases when S_1, S_2, and S_3 satisfying the conditions in Theorem 4.2 are chosen as safe-park points and nominal operation is resumed upon fault repair at $t_r = 8.5$ min and $t_r = 12.5$ min, respectively.

405.0 K) for mode 1, S_2 (0.75 kmol/m^3, 410.0 K) for mode 2, and S_3 (0.85 kmol/m^3, 412.5 K) for mode 3, for which the P matrices are $\left[\begin{smallmatrix} 5.2 & 0.16 \\ 0.16 & 0.024 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 40 & 0.33 \\ 0.33 & 0.032 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 17.5 & 0.1 \\ 0.1 & 0.01 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} 24 & 0.36 \\ 0.36 & 0.03 \end{smallmatrix}\right]$, respectively. The associated stability regions are omitted to maintain legibility in Fig. 4.5. In the predictive controller design of Section 4.2.2, a sampling time $\Delta = 0.01$ min and a prediction horizon $T = 2\Delta$ are used. Let Q_w and R_w be matrices penalizing the deviations of the state and manipulated variables from their nominal values (also in Section 4.4.2). For the primary control configuration, Q_w is an identity matrix, and R_w is a diagonal matrix with 10^4 and 5×10^{-4} as the elements on the diagonal. For the backup control configuration, Q_w remains the same, and R_w is a diagonal matrix with 10^4 and 1 as the elements on the diagonal.

Consider a scenario where the process starts from $O(1.5\,\text{kmol/m}^3, 396\,\text{K}) \in \Omega_{nom,1}$ in mode 1, and the heating valve fails at time $t_f = 0.05$ min when the process state is at $F(1.31$ kmol/m^3, 400.8 K), as shown in Fig. 4.5. If we choose a safe-park point candidate S_1' ignoring the switched nature of the process and only utilizing the safe-parking framework of [74], it results in the system being stabilized at S_1' in mode 1. The controller, however,

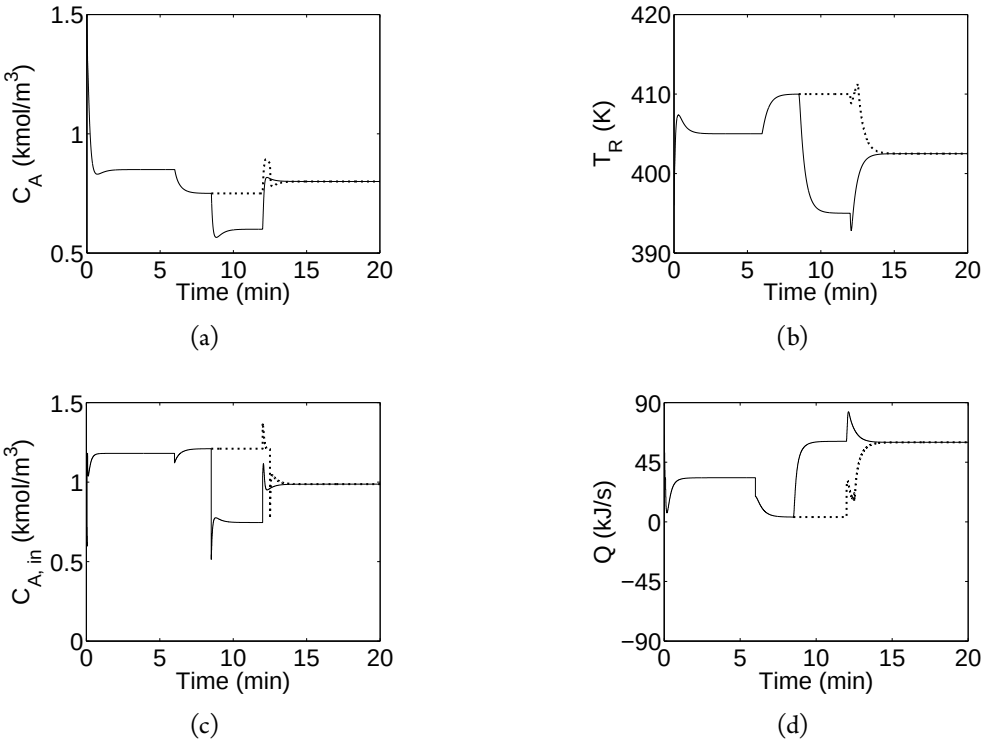

Figure 4.6: Evolution of (a, b) state and (c, d) manipulated input profiles for the switched chemical reactor example of Section 4.4.1 with a fixed schedule when the heating valve fails at $t_f = 0.05$ min. The solid and dotted lines show the cases when S_1, S_2, and S_3 satisfying the conditions in Theorem 4.2 are chosen as safe-park points and nominal operation is resumed upon fault repair at $t_r = 8.5$ min and $t_r = 12.5$ min, respectively.

fails to drive the process state to move towards S_2 after it is switched to mode 2, as shown by the dashed trajectory in Fig. 4.5. Because S_1' is not within the stability region of the safe-park point candidate S_2 for mode 2, there is no guarantee that the corresponding Lyapunov function can be made negative initially and successively using the reduced control action upon the mode transition. In contrast, if the safe-parking scheme of Theorem 4.2 is followed (S_1, S_2, and S_3 are chosen as the safe-park points simultaneously), the process is safe-parked at S_1 and S_2 successively, and nominal operation is resumed in mode 2 and continued in mode 3 if the fault is repaired at time $t_r = 8.5$ min (see the solid trajectory in Fig. 4.5). If the fault is repaired at time $t_r = 12.5$ min when the process operates in mode 3 (but before it is stabilized at S_3), the controller is immediately switched to drive the process state to move towards N_3 upon fault repair (see the dotted trajectory in Fig. 4.5), and nominal operation is resumed in mode 3. The state and input profiles for both the cases are plotted in Fig. 4.6. These results demonstrate that it is essential to account for

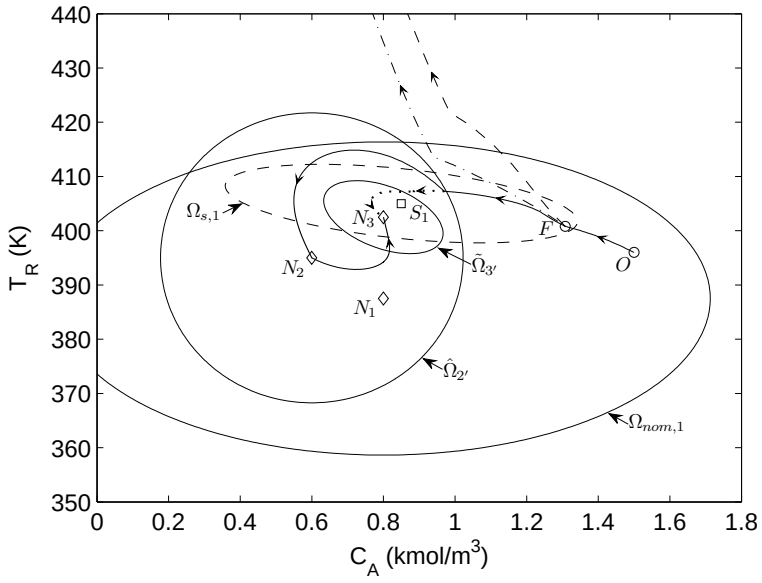

Figure 4.7: Closed-loop state trajectory for the switched chemical reactor example of Section 4.4.1 with a flexible schedule when the heating valve fails at $t_f = 0.05$ min. The dashed and dash-dotted trajectories show the cases when the process is immediately switched to modes $2'$ and $3'$, respectively, upon fault occurrence. The solid and dotted trajectories show the cases when the proposed framework is used and the process is switched to modes $2'$ and $3'$ only after it is detected that the process state enters the stability regions $\hat{\Omega}_{2'}$ at $t_1' = 0.25$ min and $\tilde{\Omega}_{3'}$ at $t_1' = 0.44$ min, respectively.

the switched nature of the system when choosing safe-park points.

To illustrate the safe-switching framework for a flexible schedule, consider nominal schedules $1 \xrightarrow{6\,\text{min}} 2' \xrightarrow{12\,\text{min}} 3 \xrightarrow{20\,\text{min}}$ end and $1 \xrightarrow{6\,\text{min}} 2 \xrightarrow{12\,\text{min}} 3' \xrightarrow{20\,\text{min}}$ end, with the flexibility of switching to and operating in any mode. The same fault scenario is considered except that it is repaired at time $t_r = 5$ min. For modes $2'$ and $3'$, the P matrices are $\left[\begin{smallmatrix} 5.6 & 0 \\ 0 & 0.0014 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 6.25 & 0.0625 \\ 0.0625 & 0.0025 \end{smallmatrix}\right]$, respectively, under the primary control configuration. The P matrix remains the same for mode $2'$ under the reduced primary control configuration, with $\hat{\Omega}_{2'}$ the stability region, and it is $\left[\begin{smallmatrix} 45 & 0.5 \\ 0.5 & 0.0276 \end{smallmatrix}\right]$ for mode $3'$ under the backup control configuration, with $\tilde{\Omega}_{3'}$ the stability region (see Fig. 4.7). Note that in the presence of the fault, nominal operation can be continued in mode $2'$ under the (reduced) primary control configuration as well as in mode $3'$ under the backup control configuration. As discussed in Remark 4.11, if we simply switch the process to mode $2'$ or $3'$ upon fault occurrence, the controller is unable to drive the process state to move towards the corresponding nominal equilibrium point (see the dashed and dash-dotted trajectories in Fig. 4.7). In contrast, nominal operation is

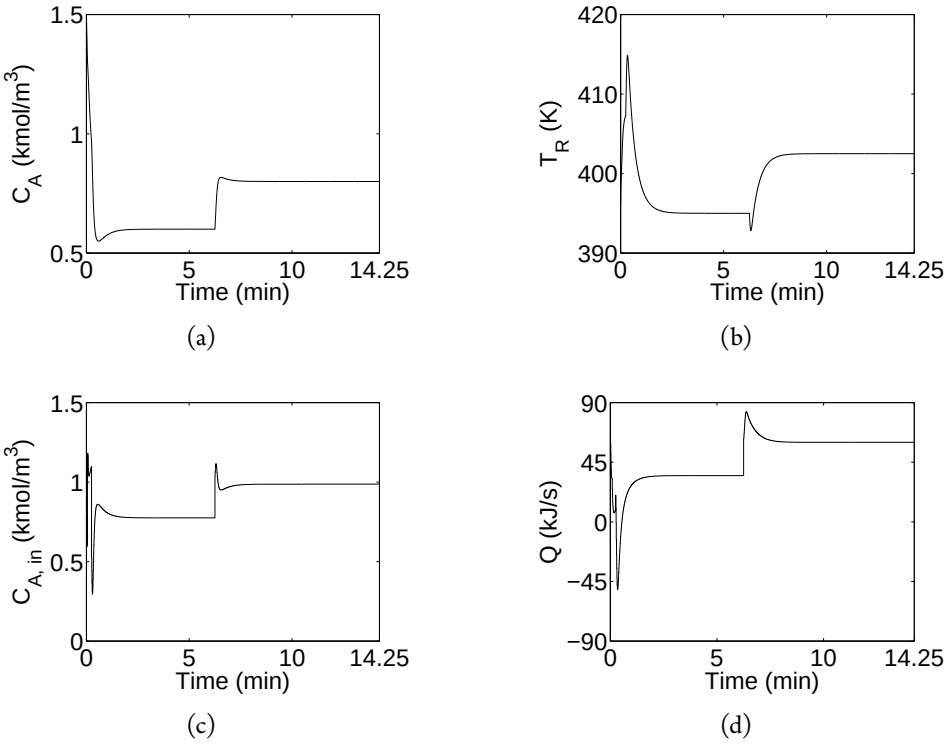

Figure 4.8: Evolution of (a, b) state and (c, d) manipulated input profiles for the switched chemical reactor example of Section 4.4.1 with a flexible schedule of $1 \xrightarrow{6\,\text{min}} 2' \xrightarrow{12\,\text{min}} 3 \xrightarrow{20\,\text{min}}$ end when the heating valve fails at $t_f = 0.05$ min. The process is switched to mode $2'$ after it is detected that the process state enters the stability region $\hat{\Omega}_{2'}$ at $t_1' = 0.25$ min.

resumed if we first drive the process state to move towards S_1 and then switch the process to mode $2'$ or $3'$ as soon as it is detected that the state enters the stability region $\hat{\Omega}_{2'}$ (at time $t_1' = 0.25$ min) or $\tilde{\Omega}_{3'}$ (at time $t_1' = 0.44$ min), as shown by the solid and dotted trajectories in Fig. 4.7. After the fault is repaired at time $t_r = 5$ min, in the case where the process is switched to mode $2'$, nominal operation in mode 3 is also achieved upon the transition to mode 3 at time $t_2' = 6.25$ min (after waiting for the designed operating time in mode $2'$), while in the case where it is switched to mode $3'$, the process finishes after the designed operating time in mode $3'$. The corresponding state and input profiles are shown in Figs. 4.8 and 4.9, respectively. Instead of operating at the safe-park point, the off-spec product is reduced by exploiting the switched nature of the process.

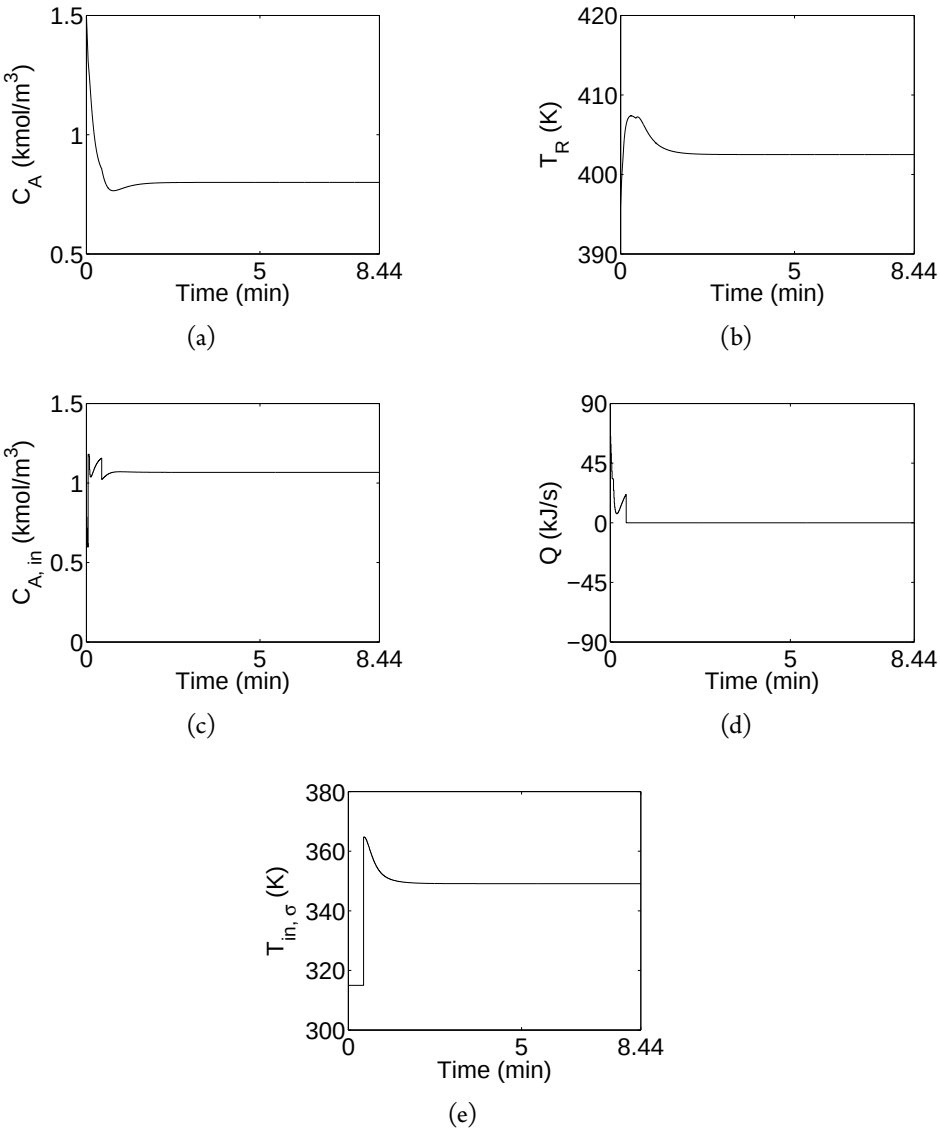

Figure 4.9: Evolution of (a, b) state and manipulated (c, d, e) input profiles for the switched chemical reactor example of Section 4.4.1 with a flexible schedule of $1 \overset{6\,\text{min}}{\longrightarrow} 2 \overset{12\,\text{min}}{\longrightarrow} 3' \overset{20\,\text{min}}{\longrightarrow}$ end when the heating valve fails at $t_f = 0.05$ min. The process is switched to mode $3'$ after it is detected that the process state enters the stability region $\tilde{\Omega}_{3'}$ at $t_1' = 0.44$ min. The backup control configuration is activated at the same time.

4.4.2 Application to an MMA Polymerization Process

Consider a nonisothermal free-radical polymerization process of MMA (studied in the context of feedforward/feedback control in [84, 119] and optimization of grade transitions in [120]):

$$\begin{aligned}
\dot{C}_m &= -\left(Z_p e^{-E_p/RT} + Z_{f_m} e^{-E_{fm}/RT}\right) C_m P_0(C_I, T) + \frac{F_m C_{m,in,\sigma} - (F_m + F_I) C_m}{V} \\
\dot{C}_I &= -Z_I e^{-E_I/RT} C_I + \frac{F_I C_{I,in} - (F_m + F_I) C_I}{V} \\
\dot{T} &= Z_p e^{-E_p/RT} C_m \frac{-\Delta H_P}{\rho_m c_p} P_0(C_I, T) - \frac{UA}{\rho_m c_p V}(T - T_j) + \frac{(F_m + F_I)(T_{in,\sigma} - T)}{V} \\
\dot{D}_0 &= \left(0.5 Z_{T_c} e^{-E_{T_c}/RT} + Z_{T_d} e^{-E_{T_d}/RT}\right) [P_0(C_I, T)]^2 + Z_{f_m} e^{-E_{fm}/RT} C_m P_0(C_I, T) \\
&\quad - \frac{(F_m + F_I) D_0}{V} \\
\dot{D}_1 &= M_m \left(Z_p e^{-E_p/RT} + Z_{f_m} e^{-E_{fm}/RT}\right) C_m P_0(C_I, T) - \frac{(F_m + F_I) D_1}{V} \\
\dot{T}_j &= \frac{F_w}{V_o}(T_{w,in} - T_j) + \frac{UA}{\rho_w c_w V_o}(T - T_j)
\end{aligned} \tag{4.10}$$

where

$$P_0(C_I, T) = \left[\frac{2 f^* C_I Z_I e^{-E_I/RT}}{Z_{T_d} e^{-E_{T_d}/RT} + Z_{T_c} e^{-E_{T_c}/RT}}\right]^{0.5}$$

C_m and C_I represent the molar concentrations of monomer and initiator, respectively, T and T_j represent the reactor and jacket temperatures, respectively, and D_0 and D_1 represent the molar and mass concentrations of dead chains, respectively. In this study, we use the number average molecular weight D_1/D_0 to characterize the polymer grade and focus on a single grade change from 2.5×10^4 kg/kmol ($\sigma = 1$) to 3.5×10^4 kg/kmol ($\sigma = 2$), with the reactor temperature maintained at 335 K, by manipulating the volumetric flow rate of the initiator $0.0007\ \text{m}^3/\text{hr} \leq F_I \leq 0.1\ \text{m}^3/\text{hr}$ and the volumetric flow rate of the cooling water $0.3\ \text{m}^3/\text{hr} \leq F_w \leq 6\ \text{m}^3/\text{hr}$, where $F_w = F_{w1} + F_{w2}$, with $0.3\ \text{m}^3/\text{hr} \leq F_{w1} \leq 4\ \text{m}^3/\text{hr}$ and $0 \leq F_{w2} \leq 2\ \text{m}^3/\text{hr}$ (two cooling valves are used).

The nominal schedule considered is $1 \xrightarrow{4\,\text{hr}} 2 \xrightarrow{10\,\text{hr}}$ end, where the inlet stream is composed of monomer with concentration $C_{m,in,1} = 6.0\,\text{kmol/m}^3$, $C_{m,in,2} = 6.5\,\text{kmol/m}^3$ and temperature $T_{in,1} = 350$ K, $T_{in,2} = 355$ K. The other process parameters can be found in [119, 120], and the steady-state values of the state and manipulated variables can be computed accordingly. Let $x_{nom,1}$ and $x_{nom,2}$ denote the nominal equilibrium points for modes

1 and 2, respectively. In the predictive controller design of Section 4.2.2, the P matrices are obtained by solving the Riccati equation for the linearized system. The sampling time $\Delta = 18$ s, the prediction horizon $T = 2\Delta$, Q_w is an identity matrix, and R_w is a diagonal matrix with 10^4 and 1 as the elements on the diagonal. To demonstrate the robustness with respect to uncertainty and measurement noise, we consider errors in the frequency factor Z_I and the heat of reaction ΔH_P of magnitude 10% and sinusoidal disturbances in the inlet monomer concentration and the temperature of the inlet streams of amplitudes 0.01 kmol/m^3 and 0.5 K, respectively, and period of oscillation of 10 minutes, as well as measurement noise of magnitude 0.1% around the nominal values. To alleviate the effect of noise, filtered measurements are used to calculate the control input.

We consider two scenarios: (1) both the cooling valves fail and revert to their fully open positions, and (2) only the valve used to control F_{w1} fails and reverts to its fully open position. In either of the two cases, the fault takes place at time $t_f = 2$ hr when the process operates at the nominal equilibrium point of mode 1, and it is repaired at time $t_r = 7$ hr. For both scenarios, the key problem is to determine the operating policy in the presence of the fault by accounting for or exploiting (if possible) the switched nature of the process to minimize off-spec product. To this end, we design safe-park point candidates S_1 and S_1' for mode 1 and S_2 for mode 2, with the number average molecular weight 24497, 24788, 34854 kg/kmol and reactor temperature 334.17, 334.59, 334.89 K, respectively.

First, we consider the scenario where both the cooling valves fail, resulting in $F_w \equiv 6$ m^3/hr. Note that while the use of stability regions (Ω) in implementing the safe-parking framework provides the necessary guarantee, the set Π which is much easier to compute (and typically larger than Ω) can be used to practically implement the proposed framework. To this end, we choose S_1 and S_2 as the safe-park points for modes 1 and 2, respectively, since $x_{nom,1}$ is in the set Π of S_1, S_1 is in the set Π of S_2, and S_2 is also in the set Π of $x_{nom,2}$. According to Theorem 4.2, the process is first safe-parked at S_1 in mode 1 and then safe-parked successively at S_2 after the mode transition. Upon fault repair, nominal operation is resumed in mode 2 using the complete control action, as shown in Fig. 4.10.

Next, we demonstrate the scenario where it is possible to continue nominal operation in another mode. To this end, consider the scenario where only the valve used to control F_{w1} fails, leading to 4 m^3/hr $\leq F_w \leq$ 6 m^3/hr. In this scenario, the proposed framework dictates safe-parking the process at S_1' in mode 1 (the set Π of S_1' includes $x_{nom,1}$ and S_1' also resides in the set Π of $x_{nom,2}$). Note that, as discussed in Remark 4.6, when there are multiple safe-park points that satisfy the requirements of Theorem 4.2 (in this case, both S_1 and S_1' are eligible), we pick a safe-park point that minimizes the deviation from the desired

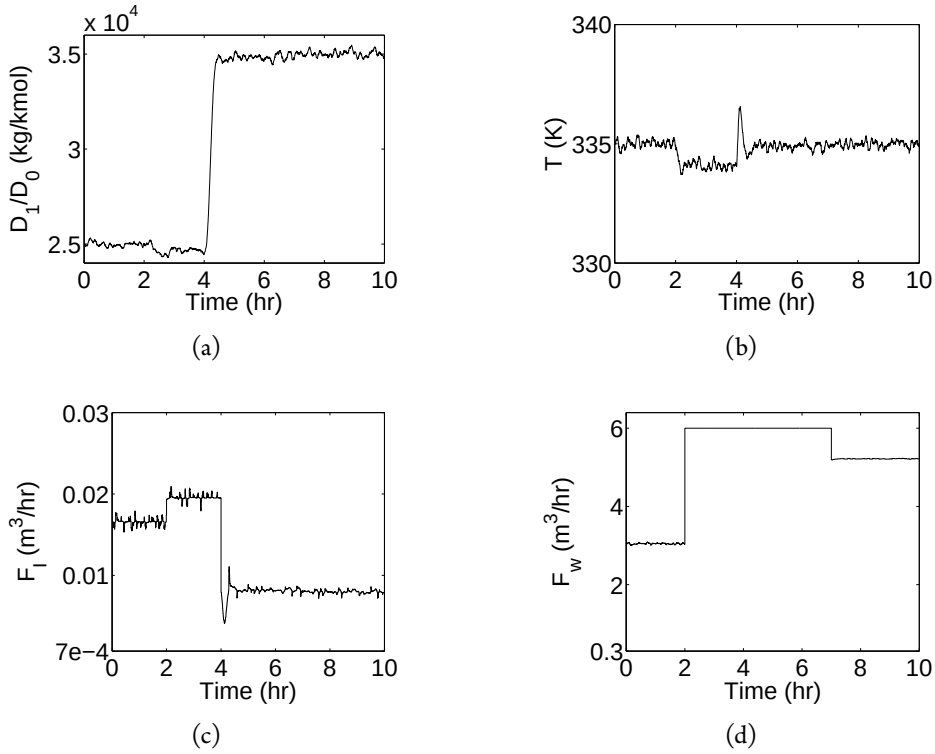

Figure 4.10: Evolution of (a, b) grade and (c, d) input profiles for the MMA polymerization process when both the cooling valves fail at $t_f = 2$ hr. The safe-parking framework of Theorem 4.2 dictates safe-parking at S_1 and then at S_2. Nominal operation is resumed in mode 2 upon fault repair at $t_r = 7$ hr.

product specifications. In this case, the point S_1' yields a product closer to the desired grade. Hence, the process is safe-parked at S_1' instead of S_1. Thereafter, when the process transits to mode 2, resumption of nominal operation is achieved, as shown in Fig. 4.11. Note that if the inlet stream of mode 2 were available earlier (i.e., the switching schedule were flexible), the proposed framework would dictate switching to mode 2 instead of safe-parking the process in mode 1 according to Theorem 4.3. In summary, the proposed framework is able to achieve safe-operation, as well as continuation of nominal operation upon or even before (when possible) fault repair for the MMA polymerization process in the presence of uncertainty and measurement noise.

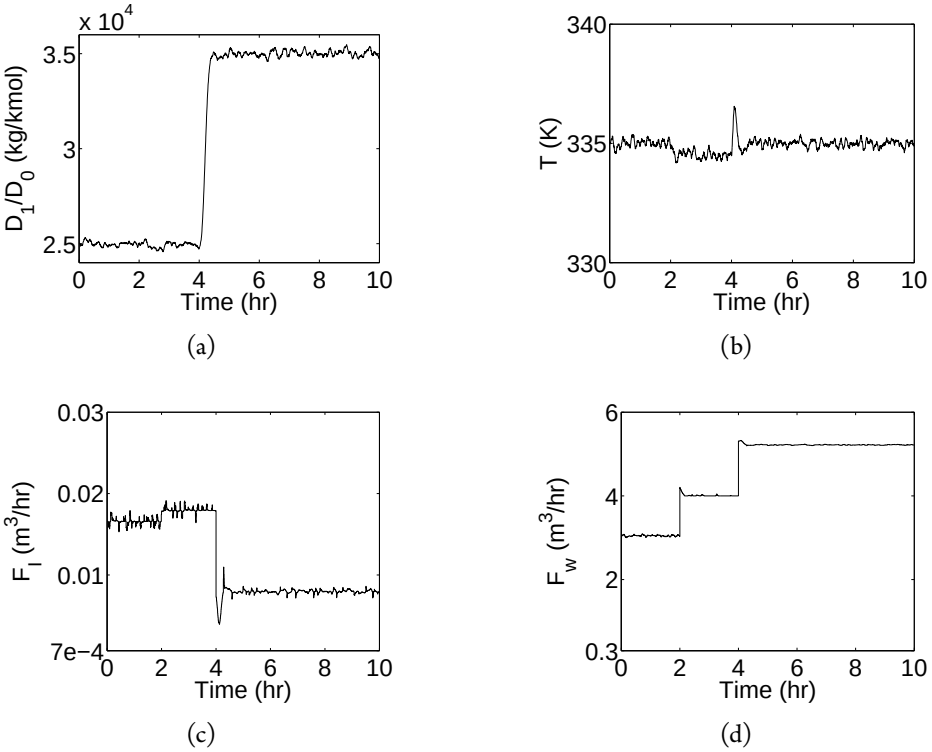

Figure 4.11: Evolution of (a, b) grade and (c, d) input profiles for the MMA polymerization process when the cooling valve used to control F_{cw1} fails at $t_f = 2$ hr. The safe-parking framework of Theorem 4.2 dictates safe-parking at S_1'. Nominal operation is resumed in mode 2 upon the mode transition at $t_1 = 4$ hr.

4.5 Conclusions

This chapter presented a safe-parking and safe-switching framework to handle actuator faults in switched nonlinear process systems subject to input constraints. The faults considered preclude the possibility of operation at the nominal equilibrium point in the active mode. Two cases were considered according to whether or not the switching schedule can be altered during the production process. For the case where the switching schedule is fixed, a safe-parking scheme was designed, which accounts for the switched nature, to operate the process at successive safe-park points as it transits to successive modes, which allow resumption of nominal operation after the fault is repaired. For the case where the switching schedule is adjustable, a safe-switching scheme was designed, which exploits the switched nature, to switch the process to a mode (if exists and available) where nominal operation can be preserved (through control structure reconfiguration when necessary) to continue nominal operation. The key ideas of the proposed framework were illustrated via a switched chemical reactor example, and the robustness with respect to uncertainty and measurement noise was demonstrated on an MMA polymerization process.

Chapter 5

Integrated FDI and Safe-Parking of Networked Nonlinear Process Systems[1]

5.1 Introduction

The previous chapter addresses the problem of safe-parking for an isolated unit by accounting for the changes in process dynamics. Most processes in chemical industries, however, use a complex integration of streams for many purposes, such as carrying the materials to multiple units or improving the heat economy of the plant (see [122] for control designs considering the networked nature of the process). The network structure of a chemical plant adds another layer of complexity in the practical implementation of the safe-parking approach. The key problem that needs to be addressed is how to wisely choose a safe-park point that can help prevent the effect of faults propagating through the network. This problem has been studied for systems with simple network structure where multiple units are connected in series (see [76]), where a region that is able to preserve nominal operation in the downstream unit is characterized for the unit where a fault takes place. The choice of a safe-park point within this region allows the continuation of nominal operation in the downstream unit. Consequently, the effect of faults will not propagate through the fur-

[1] The results in this chapter have been published in:

a. M. Du, R. Gandhi, and P. Mhaskar. An integrated fault detection and isolation and safe-parking framework for networked process systems. *Ind. & Eng. Chem. Res.*, 50:5667–5679, 2011.

b. M. Du, R. Gandhi, and P. Mhaskar. Fault detection and isolation and safe-parking of networked systems. In *Proceedings of the 2011 American Control Conference*, pages 3146–3151, San Francisco, CA, 2011.

ther downstream units. If there do not exist possible safe-park points within this region, the two units need to be safe-parked simultaneously, and the same procedure is repeated to determine whether nominal operation can be preserved in a further downstream unit. Sequentially choosing safe-park points, however, does not address the inherent interconnection among the units, which may lead to a missed opportunity of continuing nominal operation in an early unit. Furthermore, the method developed for units in series does not remain directly applicable to more complex networks with parallel and recycle structures, and no FDI designs are explicitly considered in [74–76].

Motivated by the above considerations, This chapter considers the problem of FDI and fault-handling for networked process systems subject to actuator faults. It is assumed that the failed actuator reverts to its fail-safe position and precludes the possibility of nominal operation in the affected unit. A robust FDI design is first presented, where relations between the prescribed inputs and state measurements in the absence of faults are constructed with the consideration of uncertainty. A fault is detected and isolated when the corresponding relation is violated. An algorithm is then developed to determine the units that need to be safe-parked during the fault repair period and generate possible safe-park points for the affected units. The implementation of the safe-parking techniques is triggered by the isolation of a fault, which can localize the effect of the fault in a subsystem of the networked plant. The efficacy of the integrated FDI and safe-parking framework is demonstrated on a chemical process example comprising three reactors and a separator.

The remainder of this chapter is organized as follows. Section 5.2 presents the description of the networked process systems and the problem statement, followed by a review of the safe-parking approach for FTC. Section 5.3 presents the robust FDI design. In Section 5.4, the algorithm is proposed for safe-parking of networked process systems. In Section 5.5, the simulation results are presented. Finally, Section 5.6 presents some concluding remarks.

5.2 Preliminaries

In this section, we describe the class of process systems considered, followed by a chemical process example, present the problem statement, and review the safe-parking approach for FTC.

5.2.1 Process Description

Consider a networked process system comprising M units, described by the following ordinary differential equations:

$$\begin{aligned}
\dot{x}_1 &= f_1(x_1) + G_1(x_1)(u_1 + \tilde{u}_1) + \sum_{j=2}^{M} R_{1,j}(x_1)x_j + W_1(x_1)\theta_1 \\
&\vdots \\
\dot{x}_i &= f_i(x_i) + G_i(x_i)(u_i + \tilde{u}_i) + \sum_{j=1, j\neq i}^{M} R_{i,j}(x_i)x_j + W_i(x_i)\theta_i \\
&\vdots \\
\dot{x}_M &= f_M(x_M) + G_M(x_M)(u_M + \tilde{u}_M) + \sum_{j=1}^{M-1} R_{M,j}(x_M)x_j + W_M(x_M)\theta_M
\end{aligned} \tag{5.1}$$

where $x_i = [x_{i,1}, \ldots, x_{i,n_i}]^{\mathrm{T}} \in \mathbb{R}^{n_i}$, $i \in \mathcal{M} := \{1, \ldots, M\}$ denotes the vector of state variables for the ith unit, $u_i = [u_{i,1}, \ldots, u_{i,m_i}]^{\mathrm{T}} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M}$ denotes the vector of constrained manipulated variables for the ith unit, taking values in a nonempty convex set $\mathcal{U}_i = \{u_i \in \mathbb{R}^{m_i} : u_{i,\min} \leq u_i \leq u_{i,\max}\}$, with $u_{i,\min} = [u_{i,1,\min}, \ldots, u_{i,m_i,\min}]^{\mathrm{T}}$, $u_{i,\max} = [u_{i,1,\max}, \ldots, u_{i,m_i,\max}]^{\mathrm{T}} \in \mathbb{R}^{m_i}$ the constraints on the manipulated variables, $\tilde{u}_i = [\tilde{u}_{i,1}, \ldots, \tilde{u}_{i,m_i}]^{\mathrm{T}} \in \mathbb{R}^{m_i}$ denotes the fault vector, with $u_i + \tilde{u}_i \in \mathcal{U}_i$, and $\theta_i = [\theta_{i,1}, \ldots, \theta_{i,q_i}]^{\mathrm{T}} \in \mathbb{R}^{q_i}$, $\theta_{i,\min} \leq \theta_i \leq \theta_{i,\max}$ denotes the vector of bounded uncertain variables affecting the ith unit, with $\theta_{i,\min} = [\theta_{i,1,\min}, \ldots, \theta_{i,q_i,\min}]^{\mathrm{T}}$, $\theta_{i,\max} = [\theta_{i,1,\max}, \ldots, \theta_{i,q_i,\max}]^{\mathrm{T}} \in \mathbb{R}^{q_i}$ the bounds on uncertainty. For $i = 1, \ldots, M$, the vector function $f_i(\cdot) = [f_{i,1}(\cdot), \ldots, f_{i,n_i}(\cdot)]^{\mathrm{T}}$, where $f_{i,j}(\cdot)$ denotes the jth element of $f_i(\cdot)$, $j = 1, \ldots, n_i$, and the matrix functions $G_i(\cdot) = [g_{i,1}(\cdot)^{\mathrm{T}}, \ldots, g_{i,n_i}(\cdot)^{\mathrm{T}}]^{\mathrm{T}}$, where $g_{i,j}(\cdot)$ denotes the jth row of $G_i(\cdot)$, $j = 1, \ldots, n_i$, $R_{i,j}(\cdot) = [r_{i,j,1}(\cdot)^{\mathrm{T}}, \ldots, r_{i,j,n_i}(\cdot)^{\mathrm{T}}]^{\mathrm{T}}$, where $r_{i,j,l}(\cdot)$ denotes the lth row of $R_{i,j}(\cdot)$, $l = 1, \ldots, n_i$, and $W_i(\cdot) = [w_{i,1}(\cdot)^{\mathrm{T}}, \ldots, w_{i,n_i}(\cdot)^{\mathrm{T}}]^{\mathrm{T}}$, where $w_{i,j}(\cdot)$ denotes the jth row of $W_i(\cdot)$, $j = 1, \ldots, n_i$, are assumed to be sufficiently smooth on their domains of definition. The ith row in Eq. (5.1) describes the subsystem for unit i, which is connected with units indexed by $\mathcal{M}\backslash\{i\}$ (the notation $A\backslash B$, where A and B are sets, refers to the relative complement, defined by $A\backslash B = \{x \in A : x \notin B\}$). It is assumed that the origin, i.e., $x_i = 0$, $i \in \mathcal{M}$, is the nominal equilibrium point for each subsystem under nominal conditions (i.e., $\tilde{u}_i \equiv 0$, $\theta_i \equiv 0$, and $x_j \equiv 0$ for all $j \in \mathcal{M}\backslash\{i\}$). Each unit i is controlled by a local robust controller with a stability region denoted by $\Omega_{nom,i}$ (see [75] for one example of a robust control law with a well characterized stability region), and the

state information is shared between the controllers for interconnected units. Piecewise constant control is implemented, i.e., $u(t) = u(t_k)$, for all $t \in [t_k, t_{k+1})$, where $t_k := k\Delta$, $k = 0, \ldots, \infty$, with Δ the execution period during which the input is kept constant. In this chapter, we focus on the state feedback problem, where the measurements of $x_i(t)$ for all $i \in \mathcal{M}$ are assumed to be available for all $t \geq 0$.

5.2.2 Motivating Example

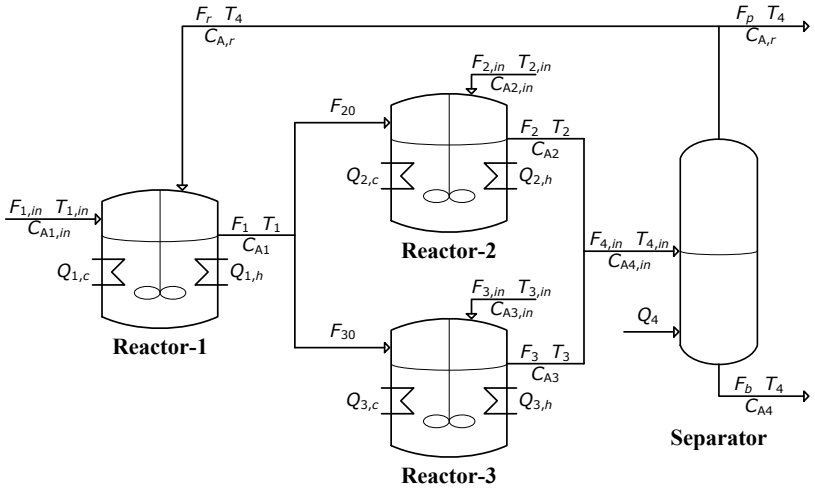

Figure 5.1: Schematic of the networked process system comprising three reactors and a separator of Section 5.2.2.

To motivate the present work, we consider a networked process system comprising three reactors and a separator with two parallel streams and a recycle stream, as shown in Fig. 5.1 (a similar example is considered in the context of distributed model predictive control [123]). In this plant, three parallel irreversible elementary exothermic reactions of the form A $\xrightarrow{k_1}$ B, A $\xrightarrow{k_2}$ U, and A $\xrightarrow{k_3}$ R take place in the reactors, where A is the reactant species, B the desired product, and U, R the undesired byproducts. The feed to reactor-i, $i = 1, 2, 3$, consists of reactant A at a flow rate $F_{i,in}$, concentration $C_{Ai,in}$, and temperature $T_{i,in}$. The outlet stream of reactor-1 at a flow rate F_1 is split into two streams such that 61.5% of the flow (F_{20}) goes to reactor-2 and the rest (F_{30}) to reactor-3. Then, the outlet streams of reactor-2 and reactor-3 go to the separator, where reactant A is separated from the products B, U, and R, and recycled back to reactor-1. It is assumed that the reactions taking place in the separator are negligible, the molecular weight of the solvent is the same as that of species A, and the products and solvent have the same volatility. Due to the nonisother-

mal nature of the reactions, each reactor is provided with two coils to add/remove heat to/from it. Under standard assumptions, the mathematical model for the process takes the following form:

Reactor-1

$$\begin{aligned}
\frac{dC_{A1}}{dt} &= \frac{F_{1,in}}{V_1}(C_{A1,in} - C_{A1}) - \sum_{j=1}^{3} R_j(C_{A1}, T_1) + \frac{F_r}{V_1}(C_{A,r} - C_{A1}) \\
\frac{dT_1}{dt} &= \frac{F_{1,in}}{V_1}(T_{1,in} - T_1) + \sum_{j=1}^{3} \frac{(-\Delta H_j)}{\rho c_p} R_j(C_{A1}, T_1) + \frac{F_r}{V_1}(T_4 - T_1) + \frac{Q_1}{\rho c_p V_1}
\end{aligned} \tag{5.2}$$

Reactor-2

$$\begin{aligned}
\frac{dC_{A2}}{dt} &= \frac{F_{2,in}}{V_2}(C_{A2,in} - C_{A2}) - \sum_{j=1}^{3} R_j(C_{A2}, T_2) + \frac{F_{20}}{V_2}(C_{A1} - C_{A2}) \\
\frac{dT_2}{dt} &= \frac{F_{2,in}}{V_2}(T_{2,in} - T_2) + \sum_{j=1}^{3} \frac{(-\Delta H_j)}{\rho c_p} R_j(C_{A2}, T_2) + \frac{F_{20}}{V_2}(T_1 - T_2) + \frac{Q_2}{\rho c_p V_2}
\end{aligned} \tag{5.3}$$

Reactor-3

$$\begin{aligned}
\frac{dC_{A3}}{dt} &= \frac{F_{3,in}}{V_3}(C_{A3,in} - C_{A3}) - \sum_{j=1}^{3} R_j(C_{A3}, T_3) + \frac{F_{30}}{V_3}(C_{A1} - C_{A3}) \\
\frac{dT_3}{dt} &= \frac{F_{3,in}}{V_3}(T_{3,in} - T_3) + \sum_{j=1}^{3} \frac{(-\Delta H_j)}{\rho c_p} R_j(C_{A3}, T_3) + \frac{F_{30}}{V_3}(T_1 - T_3) + \frac{Q_3}{\rho c_p V_3}
\end{aligned} \tag{5.4}$$

Separator

$$\begin{aligned}
\frac{dC_{A4}}{dt} &= \frac{F_b}{V_4}(C_{A4,in} - C_{A4}) + \frac{F_r + F_p}{V_4}(C_{A4,in} - C_{A,r}) \\
\frac{dT_4}{dt} &= \frac{F_{4,in}}{V_4}(T_{4,in} - T_4) + \frac{Q_4}{\rho c_p V_4} \\
C_{A4,in} &= \frac{C_{A2}(F_{2,in} + F_{20}) + C_{A3}(F_{3,in} + F_{30})}{F_{2,in} + F_{20} + F_{3,in} + F_{30}} \\
T_{4,in} &= \frac{T_2(F_{2,in} + F_{20}) + T_3(F_{3,in} + F_{30})}{F_{2,in} + F_{20} + F_{3,in} + F_{30}} \\
C_{A,r} &= \frac{\alpha C_{A4} \rho}{\rho + (\alpha - 1) C_{A4} MW}
\end{aligned} \tag{5.5}$$

where C_{Ai} is the concentration of species A, T_i is the temperature, Q_i is the rate of heat

Table 5.1: Process parameters for the networked process system of Section 5.2.2.

Parameter	Value	Unit	Parameter	Value	Unit
$T_{1,in}$	300	K	V_4	1.0	m^3
$T_{2,in}$	300	K	c_p	0.231	kJ/kg·K
$T_{3,in}$	300	K	ρ	1000.0	kg/m^3
$F_{1,in}$	5	m^3/hr	R	8.314	kJ/kmol·K
$F_{2,in}$	3.077	m^3/hr	MW	50	kg/kmol
$F_{3,in}$	1.923	m^3/hr	α	1.25	-
F_r	2	m^3/hr	$C_{A1,in,\min}$	0	$kmol/m^3$
F_p	0	m^3/hr	$C_{A1,in,\max}$	5	$kmol/m^3$
k_{10}	3.0×10^6	hr^{-1}	$Q_{1,\min}$	-1×10^5	kJ/hr
k_{20}	3.0×10^5	hr^{-1}	$Q_{1,\max}$	1×10^5	kJ/hr
k_{30}	3.0×10^5	hr^{-1}	$C_{A2,in,\min}$	2	$kmol/m^3$
E_1	5.00×10^4	kJ/kmol	$C_{A2,in,\max}$	4	$kmol/m^3$
E_2	7.53×10^4	kJ/kmol	$Q_{2,\min}$	-5×10^5	kJ/hr
E_3	7.53×10^4	kJ/kmol	$Q_{2,\max}$	2×10^5	kJ/hr
ΔH_1	-5.0×10^4	kJ/kmol	$C_{A3,in,\min}$	1.5	$kmol/m^3$
ΔH_2	-5.2×10^4	kJ/kmol	$C_{A3,in,\max}$	3.5	$kmol/m^3$
ΔH_3	-5.4×10^4	kJ/kmol	$Q_{3,\min}$	-5×10^5	kJ/hr
V_1	1.0	m^3	$Q_{3,\max}$	1×10^5	kJ/hr
V_2	0.8	m^3	$Q_{4,\min}$	-1×10^4	kJ/hr
V_3	0.5	m^3	$Q_{4,\max}$	1×10^4	kJ/hr

input, V_i is the volume, with subscript i denoting reactor-i ($i = 1, 2, 3$) or the separator ($i = 4$), $R_j(C_{Ai}, T_i) = k_{j0}e^{-E_j/RT_i}C_{Ai}$ is the reaction rate for the jth reaction in the ith reactor, $j = 1, 2, 3$, k_{j0}, E_j, ΔH_j denote the pre-exponential constant, the activation energy, and the enthalpy of the three reactions, respectively, MW is the molecular weight, c_p and ρ denote the heat capacity and the density of the fluid in the reactor, respectively, α is the relative volatility, and F_b, F_r, F_p denote the flow rates of the bottom product stream, the recycle stream, and the remaining top stream from the separator, respectively. The process parameters are given in Table 5.1.

The control objective under fault-free conditions is to maintain the concentration and temperature in each unit at their desired values. The manipulated variables for reactor-i are the concentration of species A in the feed stream, denoted by $C_{Ai,in}$, and the rate of heat input to the reactor, denoted by $Q_i = Q_{i,c} + Q_{i,h}$ with $Q_{i,c}$ and $Q_{i,h}$ representing the effects of cooling and heating, respectively. For the separator, the only manipulated variable is the rate of heat input, denoted by Q_4. The nominal values for the process state and manipulated variables can be found in Table 5.2, where N denotes the nominal equilibrium point. There exist uncertainty in parameter k_{10} of magnitude $\pm 2\%$ and sinusoidal disturbances in the

Table 5.2: Steady-state values of the state and manipulated variables for each unit in the networked process system of Section 5.2.2.

Variable	N	S_1	S_2	S_3	Unit
C_{A1}	2.3762	3.1907	2.1737	2.8876	kmol/m^3
T_1	328.03	363.54	351.76	327.20	K
C_{A2}	1.7847	1.7847	1.7847	2.1128	kmol/m^3
T_2	432.99	432.99	432.99	426.08	K
C_{A3}	1.7847	1.7847	1.7847	1.7847	kmol/m^3
T_3	432.99	432.99	432.99	432.99	K
C_{A4}	1.7206	1.7206	1.7206	1.9161	kmol/m^3
T_4	432.99	432.99	432.99	428.74	K
$C_{A1,in}$	2.5	3.75	2.25	3.125	kmol/m^3
Q_1	-2×10^4	1×10^4	1×10^4	-2×10^4	kJ/hr
$C_{A2,in}$	2.25	2.25	2.5335	2.25	kmol/m^3
Q_2	0	0	-2.3609×10^4	0	kJ/hr
$C_{A3,in}$	2.25	2.25	2.5335	1.5340	kmol/m^3
Q_3	0	0	-1.4756×10^4	516.86	kJ/hr
Q_4	0	0	0	0	kJ/hr

inlet temperature of the feed streams with an amplitude of 2 K and a period of 12 mins. Measurement noise has magnitudes of ± 0.02 kmol/m^3 in concentration and ± 0.2 K in temperature. In this example, we consider two faults in reactor-1: (1) the unavailability of the cooling stream (treated as shut) used to adjust $Q_{1,c}$, and (2) a fault in the solvent stream (treated as shut) used to adjust $C_{A1,in}$. The first fault results in $0 < Q_1 < 1 \times 10^5$ kJ/hr, and therefore precludes the possibility of nominal operation in reactor-1. A possible scenario for the second fault is that the inlet stream to reactor-1 is made up of two streams denoted by $F^1_{1,in} = 3.125$ m^3/hr and $F^2_{1,in} = 1.875$ m^3/hr, for which the concentration of species A ranges from 0 to 5 kmol/m^3. A fault that takes place in the solvent stream used to adjust the concentration of stream $F^1_{1,in}$ results in 3.125 kmol/m$^3 < C_{A1,in} < 5$ kmol/m^3, leading to off-spec product in its downstream units.

5.2.3 Problem Description

Consider the networked process system described by Eq. (5.1) with parallel and recycle streams and the failure of the mth, $m \in \{1, \ldots, m_i\}$, control actuator in unit $i \in \mathcal{M}$, which corresponds to the manipulated variable $u_{i,m}$ in Eq. (5.1). Let t_f and t_r denote the times that the fault takes place and it is repaired, respectively, which are unknown ahead of time. It is assumed that the failed actuator reverts to a so-called fail-safe position to prevent

the occurrence of hazardous situations. Examples of fail-safe positions include shut for a heating valve and completely open for a cooling valve. Under this assumption, the output of the failed actuator (or the corresponding input to the plant) is constant and known in advance, which is denoted by $\bar{u}_{i,m,f}$. Note that while the fault-handling framework is developed for fail-safe positions, it is also applicable to restrictions in the operating range (see Section 5.5 for an illustration).

The faults considered in this chapter preclude the possibility of continued nominal operation in the affected unit due to the severity of the fault. It means that there exists no available control action that can maintain operation at the nominal equilibrium point. To explain this point, we characterize the set of the feasible equilibrium points in the presence of the fault. The system of Eq. (5.1) can be written in the following compact form:

$$\dot{x} = f(x) + G(x)(u + \tilde{u}) + W(x)\theta \tag{5.6}$$

where $x = [x_1^{\mathrm{T}}, \ldots, x_M^{\mathrm{T}}]^{\mathrm{T}}$, $u = [u_1^{\mathrm{T}}, \ldots, u_M^{\mathrm{T}}]^{\mathrm{T}} \in \mathcal{U}$, $\tilde{u} = [\tilde{u}_1^{\mathrm{T}}, \ldots, \tilde{u}_M^{\mathrm{T}}]^{\mathrm{T}}$, $\theta = [\theta_1^{\mathrm{T}}, \ldots, \theta_M^{\mathrm{T}}]^{\mathrm{T}}$, and $f(\cdot)$, $G(\cdot)$, $W(\cdot)$ and $\mathcal{U}$ are appropriately defined. With $u_{i,m} + \tilde{u}_{i,m} = \bar{u}_{i,m,f}$ for all $t \in [t_f, t_r)$, the feasible equilibrium points for the entire plant are characterized by the following set:

$$C := \{x \in \mathbb{R}^{n_x} : f(x) + G(x)u = 0, u \in \mathcal{U}, u_{i,m} \equiv \bar{u}_{i,m,f}\} \tag{5.7}$$

where $n_x = \sum_{j=1}^{M} n_j$. Note that if $\bar{u}_{i,m,f} \neq 0$, the origin may not be within C for the system of Eq. (5.1). In other words, if the failed actuator is frozen at a non-nominal value, then the nominal operating point may not be an equilibrium point under faulty conditions. In this case, if the healthy actuators still tried to maintain nominal operation for the individual units, the process state would likely move away from the nominal operating point. Consequently, it may not be possible to resume nominal operation upon fault rectification, or even if it is possible, it may not be "optimal". This can result in an adverse effect on the operation for the ith unit, and due to the interconnections, on the entire plant.

The problem considered in this chapter is as follows: (1) design of a novel FDI scheme with the explicit consideration of plant-model mismatch to detect and isolate actuator faults in the individual units, and (2) design of a safe-parking framework (maintaining the process at an admissible operating point under faulty conditions) for the networked process system while accounting for the effect of complex interactions between multiple units. For the latter, the key issue is how to choose temporary operating points for the individual units such that operation can be maintained at that point under faulty conditions

(possibly maintaining on-spec product), and nominal operation can be resumed smoothly upon fault rectification.

5.2.4 Fault Detection and Isolation for Nonlinear Process Systems

The key (direct or indirect) assumption in the design of any FDI filter is the existence of a state variable that is directly and uniquely affected by a potential fault. In other words, only one actuator is used to directly regulate a state variable, which is often the case in practice (e.g., due to economic considerations). This is formalized in Assumption 5.1 below.

Assumption 5.1. [27] Consider the system of Eq. (5.1). Then for every input $u_{i,m}$, $i = 1, \ldots, M$, $m = 1, \ldots, m_i$, there exists a state $x_{i,n}$, $n \in \{1, \ldots, n_i\}$ such that with $x_{i,n}$ as an output, the relative degree of $x_{i,n}$ with respect to $u_{i,m}$ and only with respect to $u_{i,m}$ is equal to 1.

Under Assumption 5.1, the FDI design in [27] builds dedicated filters for each possible fault to detect and isolate faults. While it can in principle account for uncertainty by choosing appropriate thresholds, one of the contributions of the present work is the explicit consideration of uncertainty in the FDI design.

5.2.5 Safe-Parking Approach for Fault-Tolerant Control

In this section, we briefly review the safe-parking framework for an isolated unit [74] and its extension to a units in series setting [76]. Note that these results assume the existence of an FDI scheme. Let t_d denote the time that a fault is detected and isolated. Given the problem scenario, the safe-parking approach prescribes the operating policy for the process over $[t_d, t_r)$.

First, we consider an isolated unit indexed by i in the system of Eq. (5.1), e.g., it is the only unit or there are no other units following it (so the effect of the fault will not propagate through the network), and an actuator fault, which corresponds to the mth manipulated variable for unit i as described in Section 5.2.3. The key idea of safe-parking is to stabilize the faulty process at an appropriate temporary operating point (which is called a safe-park point if certain conditions are satisfied) chosen such that if the controller is switched to stabilize the process at this point, then the process state always evolves within the stability region of the nominal equilibrium point during fault rectification. For an isolated unit, the

requirements for a safe-park point are as follows [74]: (1) the safe-park point should be a feasible equilibrium point subject to the fault, (2) it should be possible to drive the process to the safe-park point from the time that a fault is detected and isolated, i.e., the process state at t_d should be within the stability region of the safe-park point, which we denote by $\Omega_{s,i}$, and (3) it should be possible to resume nominal operation after the fault is rectified, i.e., the safe-park point should be within the stability region of the nominal equilibrium point ($\Omega_{nom,i}$). The first and third conditions require that the safe-park point be chosen from the following set:

$$C_i := \left\{ x_i \in \mathbb{R}^{n_i} : f_i(x_i) + G_i(x_i)u_i = 0, u_i \in \mathcal{U}_i, u_{i,m} = \bar{u}_{i,m,f}, x_i \in \Omega_{nom,i} \right\} \tag{5.8}$$

which is called the candidate safe-park set for unit i (subject to the stability region $\Omega_{nom,i}$).

The safe-parking framework for an isolated unit is extended to consider multiple units in series [76]. Suppose that units j and $j+1$ are connected for $j = 1, \ldots, M-1$. The key idea here is to determine whether there exist admissible values of the manipulated variables in the downstream unit which can resist the effect of safe-parking the faulty unit i. To determine whether nominal operation can be preserved in its downstream unit, a set D_i is defined for unit i such that if unit i is stabilized at a point $x_i \in D_i$, then nominal operation can be preserved in unit $i+1$ and vice versa:

$$D_i = \{ x_i \in \mathbb{R}^{n_i} : f_{i+1}(0) + G_{i+1}(0)u_{i+1} + R_{i+1,i}(0)x_i = 0, u_{i+1} \in \mathcal{U}_{i+1} \} \tag{5.9}$$

Thus, if $C_i \cap D_i \neq \varnothing$, then nominal operation can be preserved in unit $i+1$ by choosing a safe-park point from $C_i \cap D_i$. If $C_i \cap D_i = \varnothing$, i.e., there does not exist a safe-park point candidate that allows nominal operation in the downstream unit, the faulty unit and the downstream unit should be safe-parked simultaneously. For this case, we choose a safe-park point candidate for unit i, and proceed to characterize the set D_{i+1} for unit $i+1$, with unit i operating at the chosen point, to determine if nominal operation can be preserved in unit $i+2$. If nominal operation can be preserved in unit $i+2$, we just need to safe-park units i and $i+1$. Otherwise, the same procedure is repeated for the remaining downstream units. Note again that such a sequential procedure, developed for units in series, does not remain directly applicable to complex interconnections such as parallel and recycle streams.

5.3 Robust Fault Detection and Isolation Design

In this section, we design a robust FDI scheme for the individual units in the plant of Eq. (5.1), for which Assumption 5.1 holds. The key idea of the proposed design is to construct relations between the prescribed inputs and state measurements in the absence of faults by using the process model, while accounting for uncertainty. A fault is detected and isolated when the corresponding relation is violated. To this end, consider the ordinary differential equation that describes the evolution of the nth state for the ith unit:

$$\dot{x}_{i,n} = f_{i,n}(x_i) + g_{i,n,m}(x_i)(u_{i,m}(t) + \tilde{u}_{i,m}(t)) + \sum_{j=1, j\neq i}^{M} r_{i,j,n}(x_i)x_j + w_{i,n}(x_i)\theta_i(t) \tag{5.10}$$

where $g_{i,n,m}(\cdot)$ is the mth element of $g_{i,n}(\cdot)$. As piecewise constant control is implemented, if $\tilde{u}_{i,m}(t) = 0$ (i.e., in the absence of the fault $\tilde{u}_{i,m}$) for all $t \in [t_k, t_{k+1})$, we have

$$\dot{x}_{i,n} = f_{i,n}(x_i) + g_{i,n,m}(x_i)u_{i,m}(t_k) + \sum_{j=1, j\neq i}^{M} r_{i,j,n}(x_i)x_j + w_{i,n}(x_i)\theta_i(t) \tag{5.11}$$

for $t \in [t_k, t_{k+1})$. Integrating both sides of Eq. (5.11) over (t_k, t_{k+1}) gives

$$x_{i,n}(t_{k+1}) = x_{i,n}(t_k) + \int_{t_k}^{t_{k+1}} \left[f_{i,n}(x_i) + g_{i,n,m}(x_i)u_{i,m}(t_k) + \sum_{j=1, j\neq i}^{M} r_{i,j,n}(x_i)x_j + w_{i,n}(x_i)\theta_i(t) \right] dt \tag{5.12}$$

Rearranging Eq. (5.12) yields

$$\bar{w}_{i,n}(k) = x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{g}_{i,n,m}(k)u_{i,m}(t_k) \tag{5.13}$$

where $\bar{f}_{i,n}(k) = \int_{t_k}^{t_{k+1}} \left[f_{i,n}(x_i) + \sum_{j=1, j\neq i}^{M} r_{i,j,n}(x_i)x_j \right] dt$, $\bar{g}_{i,n,m}(k) = \int_{t_k}^{t_{k+1}} g_{i,n,m}(x_i)dt$, and $\bar{w}_{i,n}(k) = \int_{t_k}^{t_{k+1}} w_{i,n}(x_i)\theta_i(t)dt$.

Since the exact value of $\bar{w}_{i,n}(k)$ cannot be computed due to the presence of the uncertain variables, Eq. (5.13) cannot be directly used for FDI. However, the lower and upper bounds on $\bar{w}_{i,n}(k)$ can be computed by using the known bounds on the uncertain variables. To this end, let $\bar{w}_{i,n,l}(k)$ and $\bar{w}_{i,n,u}(k)$ denote the lower and upper bounds on $\bar{w}_{i,n}(k)$, respectively. Then, we have $\bar{w}_{i,n,l}(k) = \int_{t_k}^{t_{k+1}} w_{i,n}(x_i)\theta_{i,l}(t)dt$

and $\bar{w}_{i,n,u}(k) = \int_{t_k}^{t_{k+1}} w_{i,n}(x_i)\theta_{i,u}(t)dt$, where $\theta_{i,l}(t) = [\theta_{i,1,l}(t), \ldots, \theta_{i,q_i,l}(t)]^{\mathrm{T}}$ and $\theta_{i,u}(t) = [\theta_{i,1,u}(t), \ldots, \theta_{i,q_i,u}(t)]^{\mathrm{T}}$, with $\theta_{i,q,l}(t) = \begin{cases} \theta_{i,q,\max}, & \text{if } w_{i,n}(x_i) \leq 0 \\ \theta_{i,q,\min}, & \text{if } w_{i,n}(x_i) > 0 \end{cases}$ and $\theta_{i,q,u}(t) = \begin{cases} \theta_{i,q,\min}, & \text{if } w_{i,n}(x_i) \leq 0 \\ \theta_{i,q,\max}, & \text{if } w_{i,n}(x_i) > 0 \end{cases}$, $q = 1, \ldots, q_i$. Therefore, in the absence of the fault $\tilde{u}_{i,m}$, the following inequality holds

$$\bar{w}_{i,n,l}(k) \leq x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{g}_{i,n,m}(k)u_{i,m}(t_k) \leq \bar{w}_{i,n,u}(k) \tag{5.14}$$

Note that $\bar{g}_{i,n,m}(k) \neq 0$ because $g_{i,n,m}(\cdot) \neq 0$ under Assumption 5.1 and $g_{i,n,m}(\cdot)$ is continuous. This allows us to compute the lower and upper bounds on $u_{i,m}(t_k)$ from those on $\bar{w}_{i,n}(k)$. To this end, let $u_a = [x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{w}_{i,n,l}(k)]/\bar{g}_{i,n,m}(k)$ and $u_b = [x_{i,n}(t_{k+1}) - x_{i,n}(t_k) - \bar{f}_{i,n}(k) - \bar{w}_{i,n,u}(k)]/\bar{g}_{i,n,m}(k)$. It follows from Eq. (5.14) and the physical constraints on the inputs that

$$u_{i,m,l}(k) \leq u_{i,m}(t_k) \leq u_{i,m,u}(k) \tag{5.15}$$

where $u_{i,m,l}(k) = \max\{u_a, u_{i,m,\min}\}$, $u_{i,m,u}(k) = \min\{u_b, u_{i,m,\max}\}$ if $\bar{g}_{i,n,m}(k) < 0$, and $u_{i,m,l}(k) = \max\{u_b, u_{i,m,\min}\}$, $u_{i,m,u}(t_k) = \min\{u_a, u_{i,m,\max}\}$ if $\bar{g}_{i,n,m}(k) > 0$. Since Eq. (5.15) is derived by assuming $\tilde{u}_{i,m}(t) = 0$ for all $t \in [t_k, t_{k+1})$, it follows from Eq. (5.10) that the only way that Eq. (5.15) is violated is when a fault of $\tilde{u}_{i,m}$ takes place. Therefore, if $u_{i,m}(t_k)$ breaches its lower bound $u_{i,m,l}(k)$ or upper bound $u_{i,m,u}(k)$, which can be verified through Eq. (5.15), then a fault associated with $u_{i,m}$ (i.e., the mth input to the ith unit) is detected and isolated simultaneously.

Remark 5.1. The proposed FDI design explicitly accounts for the presence of uncertainty. In particular, it requires, at each discrete time, evaluating whether there exist possible uncertainty realizations such that the value of the process state at the end of the evaluation interval could be reached if there were no faults taking place. A fault is declared only when such realizations do not exist for bounded uncertain variables, i.e., when Eq. (5.14) or (5.15) is violated. Therefore, it is robust in the sense that there will be no false alarms caused by uncertainty in the absence of faults. It should be noted that less severe faults that do not lead to the violation of Eq. (5.15) may be handled as disturbances via the inherent robustness of the controller design and would not lead to instability of the closed-loop system.

Remark 5.2. Note that in principle, Eq. (5.11) could be used to directly perform FDI by estimating the derivatives of the state variables. However, differentiating noisy measurements can amplify the measurement noise and lead to increased false alarms. In contrast,

the proposed FDI design relies on integrating the system equations, which is less sensitive to measurement noise. Note also that for the case where the outputs of the (healthy or faulty) actuators are piecewise constant, Eq. (5.15) provides the lower and upper bounds on the actual inputs as well. However, the idea of the proposed scheme still provides sufficient conditions to perform FDI for the case where the implemented control is not piecewise constant due to the fault. Finally, this approach does not require (or assume) that the faulty vector of the control actuators be constant; that is, the method is applicable to time-varying faults.

5.4 Safe-Parking of Networked Process Systems with Parallel and Recycle Streams

In this section, we propose a safe-parking framework for the networked process system of Eq. (5.1) with parallel and recycle streams. In particular, we determine the units that need to be operated at an appropriate temporary operating point before the fault is repaired. Note that the inlet conditions to faulty unit i may change (to non-nominal conditions) due to the presence of recycle streams. This happens when nominal operation cannot be preserved in the immediately upstream unit(s) of the faulty unit, which makes sequentially determining the units that have to be safe-parked and designing safe-park point candidates for those units ineffective. On the other hand, simply safe-parking all the units in the networked plant in the absence of a systematic procedure to evaluate the necessity of safe-parking a particular unit may lead to a missed opportunity of nominal operation (and possibly the associated off-spec product) in some units.

In the safe-parking design, we consider potential faulty scenarios with one actuator fault taking place (see Remark 5.3 for a discussion on the generalization to handle multiple faults). Let N_f denote the number of faulty scenarios under consideration and $\mathcal{N} = \{1, \ldots, N_f\}$ denote the index set for these faults. We use $\mathcal{J}_p$ to record the indices for the units that have to be safe-parked simultaneously for the pth fault, where $p \in \mathcal{N}$, which is initialized to be $\{i\}$ and updated by adding necessary entries. The determination of $\mathcal{J}_p$ is achieved by handling parallel and recycle streams alternatively. To facilitate the analysis, we consider a subsystem of Eq. (5.1), which comprises K units indexed by a set

$\mathcal{K} = \{i_1, \ldots, i_K\} \subseteq \mathcal{M}$ and described as follows (under nominal conditions):

$$\begin{aligned} \dot{x}_{i_1} &= f_{i_1}(x_{i_1}) + G_{i_1}(x_{i_1})u_{i_1} + \sum_{v=i_2}^{i_K} R_{i_1,v}(x_{i_1})x_v \\ &\vdots \\ \dot{x}_{i_K} &= f_{i_K}(x_{i_K}) + G_{i_K}(x_{i_K})u_{i_K} + \sum_{v=i_1}^{i_{K-1}} R_{i_K,v}(x_{i_K})x_v \end{aligned} \tag{5.16}$$

The above equation can be written into the following compact form:

$$\dot{x}_{\mathcal{K}} = f_{\mathcal{K}}(x_{\mathcal{K}}) + G_{\mathcal{K}}(x_{\mathcal{K}})u_{\mathcal{K}} \tag{5.17}$$

where $x_{\mathcal{K}} = [x_{i_1}^{\mathrm{T}}, \ldots, x_{i_K}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{n_{\mathcal{K}}}$, with $n_{\mathcal{K}} = \sum_{v=i_1}^{i_K} n_v$, $u_{\mathcal{K}} = [u_{i_1}^{\mathrm{T}}, \ldots, u_{i_K}^{\mathrm{T}}]^{\mathrm{T}} \in \mathcal{U}_{\mathcal{K}} := \prod_{v\in\mathcal{K}} \mathcal{U}_v$, and $f_{\mathcal{K}}(\cdot)$, $G_{\mathcal{K}}(\cdot)$ are appropriately defined.

To account for parallel streams, let $\mathcal{P}_j$ be an index set for the identified units that need to be safe-parked in the same parallel structure as unit j. Note that the parallel structure is defined from the perspective of the downstream unit. For example, if the streams out of two units go to the same downstream unit, then we say these units are in the same parallel structure. We explore each unit immediately downstream of subsystem $\mathcal{P}_j$ and determine if nominal operation can be preserved by safe-parking units $\mathcal{P}_j$. To this end, consider units indexed by $\mathcal{P}_j$ and a unit l, which is a unit immediately downstream of the subsystem $\mathcal{P}_j$, as shown in the example of Fig. 5.2(a), where it is assumed that a fault takes place in unit a and units a, j, and b have to be safe-parked simultaneously. To illustrate the key idea of the proposed algorithm, we assume that it has not been determined that if nominal operation can be preserved in unit l by safe-parking part of the units in $\mathcal{P}_j$ before the exploration of unit l. We define $D_{j,l}$ as a region such that if units $\mathcal{P}_j$ operate at an equilibrium point within $D_{j,l}$, nominal operation in unit l can be preserved, which is computed as follows:

$$D_{j,l} = \left\{ x_{\mathcal{P}_j} \in \mathbb{R}^{n_{\mathcal{P}_j}} : f_l(0) + G_l(0)u_l + \sum_{v\in\mathcal{P}_j} R_{l,v}(0)x_v = 0, u_l \in \mathcal{U}_l \right\} \tag{5.18}$$

Consider the case where the combined stream out of units $\mathcal{P}_j$ is split into streams going to the downstream units. Let $\mathcal{I}_j$ denote the index set for the units that are immediately downstream of those indexed by $\mathcal{P}_j$. For instance, $\mathcal{I}_1 = \{2, 3\}$ in the motivating example. Let $\tilde{D}_j$ denote the intersection of $D_{j,l}$ for all $l \in \mathcal{L}_j \subseteq \mathcal{I}_j$, where $\mathcal{L}_j$ is defined as an index set for the units immediately downstream of those indexed by $\mathcal{P}_j$ in which nominal operation can be

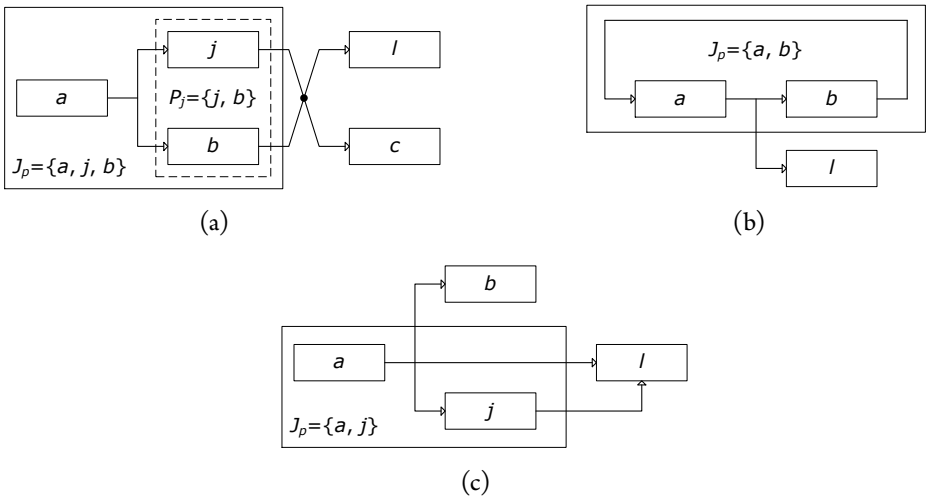

Figure 5.2: Schematics illustrating the off-line design algorithm of the safe-parking approach for networked process systems, where a fault takes place in unit *a*.

preserved. It may happen that the intersection of $D_{j,l}$ for all $l \in \mathcal{I}_j$ is empty, depending on the system dynamics of the downstream units. In that case, we have to preserve nominal operation for the units with higher priorities.

Whenever a new $D_{j,l}$ is generated, we need to verify if there exist safe-park point candidates such that nominal operation can be preserved in unit l. We use $\mathcal{E}_p$ to record the indices of the units for which there exists at least one immediately downstream unit where nominal operation can be preserved (i.e., there exist safe-park point candidates for some units $\mathcal{P}_j$ that reside within $\tilde{D}_j$). We first compute the feasible equilibrium points subject to the reduced control action for the subsystem of Eq. (5.16) with $\mathcal{K} = \mathcal{J}_p$ as follows:

$$C_{\mathcal{J}_p} = \left\{ x_{\mathcal{J}_p} \in \mathbb{R}^{n_{\mathcal{J}_p}} : \begin{array}{l} f_{\mathcal{J}_p}(x_{\mathcal{J}_p}) + G_{\mathcal{J}_p}(x_{\mathcal{J}_p}) u_{\mathcal{J}_p} = 0, u_{\mathcal{J}_p} \in \mathcal{U}_{\mathcal{J}_p}, u_{i,m} \equiv \bar{u}_{i,m,f}, \\ x_v \in \Omega_{nom,v} \text{ for all } v \in \mathcal{J}_p, x_{\mathcal{P}_v} \in \tilde{D}_v \text{ for all } v \in \mathcal{E}_p \end{array} \right\} \tag{5.19}$$

The component equilibrium points are chosen as safe-park point candidates for subsystem $\mathcal{P}_j$, which are denoted by set C_j. If $C_j \cap D_{j,l} \neq \varnothing$, then there exist safe-park point candidates such that nominal operation can be preserved in unit l. For this case, we add $\mathcal{P}_j$ to $\mathcal{E}_p$ and l to $\mathcal{L}_j$, without further exploring the downstream units of unit l. If $C_j \cap D_{j,l} = \varnothing$, we need to safe-park unit l as well and therefore add l to $\mathcal{J}_p$. For the units where nominal operation cannot be preserved, we further explore the downstream units for each of them by following the above procedure.

As the exploration proceeds, a recycle stream is detected when a downstream unit, indexed by v, of the unit under consideration, indexed by j, is identified such that it has been determined to be safe-parked (i.e. there exists a $v \in \mathcal{I}_j$ such that $v \in \mathcal{J}_p$) and there exists a path starting from unit v and ending at it along the streams connecting the units $\mathcal{J}_p$. Since it has been determined that unit v has to be safe-parked, we do not need to implement the same procedure as that for the handling of parallel streams. Note that in this case, however, it may not be true that nominal operation can still be preserved in units $\mathcal{L}_v$ (the set determined by following the procedure for parallel streams) for all $v \in \mathcal{E}_p$ due to the reason discussed at the beginning of this section. To solve this problem, we treat units $\mathcal{J}_p$ as a subsystem and examine (or reexamine) if nominal operation can be preserved in each unit downstream of this subsystem (downstream units of those indexed by $\{v \in \mathcal{J}_p : \mathcal{I}_v \backslash \mathcal{J}_p \neq \varnothing\}$, excluding those indexed by $\mathcal{J}_p$ at the time when a recycle stream is detected) by following the method developed for parallel streams to maximize the possibility of nominal operation in individual units. The exploration terminates when nominal operation can be preserved in all the downstream units of the subsystem $\mathcal{J}_p$ or this subsystem has no downstream units. The above procedure can be illustrated by the example of Fig. 5.2(b), where a fault takes place in unit a. Following the procedure for parallel streams, we explore units b and l downstream of unit a with the assumption of nominal inlet conditions to unit a. Suppose that unit b has to be safe-parked, with nominal operation preserved in unit l. A recycle stream is detected as we proceed from unit b along the network. Since safe-parking unit b leads to changes in the inlet conditions to unit a, we reexamine if nominal operation can still be preserved in unit l, which is the downstream unit of the subsystem $\mathcal{J}_p = \{a, b\}$.

Finally, we discuss the case where it has been determined that whether nominal operation can be preserved in unit l by safe-parking part of the units in $\mathcal{P}_j$ before the exploration of unit l (in the context of parallel streams). This scenario can be illustrated by Fig. 5.2(c). Assume a fault takes place in unit a. By following the proposed procedure, we examine if nominal operation can be preserved in its downstream units b, l, and j, respectively. Assume it is determined that nominal operation can be preserved in units b and l, and we need to safe-park unit j. Next, we explore the downstream unit of unit j, which is unit l. Note that it has been determined once that if nominal operation can be preserved in unit l by safe-parking unit a. At that time, it was assumed that the outlet stream of unit j is at its nominal conditions. Therefore, when units a and j are safe-parked simultaneously, it may not be true that nominal operation can still be preserved in unit l. For such a case, we can exploit the same procedure as that for the handling of recycle streams to reexamine if nominal operation can be preserved in the downstream units of subsystem $\mathcal{J}_p$ (e.g.,

$\mathcal{J}_p = \{a, j\}$) when it is necessary.

After the units that need to be safe-parked are identified, a bank of safe-park point candidates for the subsystem $\mathcal{J}_p$ can be generated according to Eq. (5.19). In contrast to the results in [76], we use the component equilibrium points of those in $C_{\mathcal{J}_p}$ for each unit as the safe-park point candidates for the individual units. The stability region of the safe-park point candidate for each unit is then computed by using the steady-state values of the upstream units and treating the deviations of the inlet conditions from their steady-state values as disturbances. All of the above calculations can be conducted off-line, with the safe-park point candidates and their associated stability regions for each potential fault stored in a database. The off-line design of the safe-parking framework for the networked process system of Eq. (5.1) is formalized in Algorithm 5.1 below (see Section 5.5 for an illustration).

Algorithm 5.1. This algorithm describes the off-line design of the safe-parking framework for the networked process system of Eq. (5.1).

1. Design a local controller for each unit, indexed by $j \in \mathcal{M}$, and characterize the stability region of the corresponding nominal equilibrium point, denoted by $\Omega_{nom,j}$. Let $\mathcal{Q} = \mathcal{N}$.

2. Pick p from $\mathcal{Q}$ and remove p from $\mathcal{Q}$. Let $\mathcal{S} = \mathcal{J}_p = \{i\}$ and $\mathcal{E}_p = \varnothing$.

   (a) If $\mathcal{S} \neq \varnothing$, pick $j \in \mathcal{S}$ and remove $\mathcal{P}_j$ from $\mathcal{S}$, else go to Step 3.

   (b) If no recycle stream is detected, let $\mathcal{T} = \mathcal{I}_j \backslash \mathcal{J}_p$, else let $\mathcal{L}_v = \varnothing$ for all $v \in \mathcal{E}_p$, $\mathcal{E}_p = \varnothing$, $\mathcal{S} = \{v \in \mathcal{J}_p : \mathcal{I}_v \backslash \mathcal{J}_p \neq \varnothing\}$, and go to Step 2a.

   (c) If $\mathcal{T} \neq \varnothing$, characterize $D_{j,l}$ for units $\mathcal{P}_j$ and some $l \in \mathcal{T}$, as defined in Eq. (5.18), and remove l from $\mathcal{T}$, else go to Step 2a.

   (d) If $C_j \cap D_{j,l} \neq \varnothing$, add $\mathcal{P}_j$ to $\mathcal{E}_p$ and l to $\mathcal{L}_j$ (initialized as $\varnothing$), else add l to $\mathcal{S}$ and $\mathcal{J}_p$. Go to Step 2c.

3. Generate safe-park point candidates $x_{s,j}$ for each unit $j \in \mathcal{J}_p$ according to Eq. (5.19).

4. Characterize the stability regions, denoted by $\Omega_{s,j}$, for all the safe-park point candidates $x_{s,j}$.

5. If $\mathcal{Q} \neq \varnothing$, repeat Step 2.

Remark 5.3. In the off-line design algorithm, while we focus on the occurrence of one actuator fault, this methodology can be generalized to handle multiple faults (possibly in different units in the context of a networked plant) that take place simultaneously or sequentially by considering the combination of fail-safe positions. While the number of potential faulty scenarios theoretically increase in a combinatorial manner as the number of actuator faults considered increases, we first note that for realistic situations, where one, two or even three actuators fail simultaneously, the design procedure can exploit computing techniques such as parallel processing to mitigate the increased computational load. We also note that the simultaneous failure of several actuators would likely necessitate plant shutdown in any case. The proposed safe-parking method would serve the purpose for most commonly encountered faulty scenarios.

Beyond the off-line design of the safe-parking approach, we also consider the on-line implementation problem for FDI and safe-parking. In particular, as the process evolves a dedicated (binary) residual for each input is generated at each discrete time, which is denoted by $\text{Res}_{u_{i,j}}(k)$. The residual is defined such that if $u_{i,j}(k) \notin [u_{i,j,l}(k), u_{i,j,u}(k)]$, $\text{Res}_{u_{i,j}}(k) = 1$ and otherwise $\text{Res}_{u_{i,j}}(k) = 0$. A fault is declared when a non-zero residual is generated at successive n_d steps, where n_d is picked to prevent false alarms due to measurement noise. Upon FDI of a fault, we search over the results of the off-line design to choose safe-park points for the units which have to be operated at a temporary operating point during fault rectification (i.e., units indexed by $\mathcal{J}_p$ if the pth fault takes place). We stabilize these units at safe-park points, while stabilizing the remaining units at nominal equilibrium points. If the faulty scenario has not been considered at the off-line design stage (e.g., several actuators fail simultaneously), we shut down the process to prevent further failures and safety hazards. This is formalized in the on-line implementation algorithm below.

Algorithm 5.2. This algorithm describes the on-line implementation of the FDI scheme of Section 5.3 and the safe-parking framework for the networked process system of Eq. (5.1).

1. At time t_{k+1}, $k = 0, \ldots, \infty$, for each unit $i \in \mathcal{M}$, compute $u_{i,j,l}(k)$ and $u_{i,j,u}(k)$, $j = 1, \ldots, m_i$.

2. Let
$$\text{Res}_{u_{i,j}}(k) := \begin{cases} 1, & \text{if } u_{i,j}(k) \notin [u_{i,j,l}(k), u_{i,j,u}(k)] \\ 0, & \text{otherwise} \end{cases} \tag{5.20}$$
If $\text{Res}_{u_{i,j}}(l) = 1, l = k+1-n_d, \ldots, k$, the fault is detected, isolated, and confirmed at time $t_d = t_{k+1}$. Otherwise, repeat Step 1.

3. Select the component equilibrium point for each unit $j \in \mathcal{J}_p$ from $C_{\mathcal{J}_p}$ such that $x_j(t_d) \in \Omega_{s,j}$.

4. Stabilize the units at safe-park points and nominal equilibrium points as determined by the off-line design. After fault rectification, resume nominal operation and repeat Step 1.

5.5 Simulation Example

Consider the process comprising three reactors and a separator, as introduced in Section 5.2.2. First, we design a Lyapunov-based robust model predictive controller [75] and characterize the stability region of the nominal equilibrium point for each unit (see Step 1 in Algorithm 5.1). To this end, the bounds on uncertainty in k_{10} are assumed to be $\pm 3\%$ and the disturbances in the inlet temperature of the feed streams are considered to be bounded between ± 5 K. A quadratic Lyapunov function of the form $V_i = x_i^{\mathrm{T}} P_i x_i$, where P_i is a positive definite matrix, is used to design the local controller and to characterize the stability region. For the sake of simplicity, the same value of $P_i = \left[\begin{smallmatrix} 4\times 10^2 & 0 \\ 0 & 4 \end{smallmatrix}\right]$ is used in the controller design. However, it should be noted that in general different values of P_i can be used in the controller design for the nominal equilibrium point and safe-park point candidates. The control execution period is chosen as $\Delta = 1.5$ min and a two-step prediction horizon is used. The matrix used to penalize the deviations of the state variables is $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 5\times 10 \end{smallmatrix}\right]$ for each unit, and those for the input variables are $\left[\begin{smallmatrix} 5\times 10^2 & 0 \\ 0 & 5\times 10^{-7} \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1\times 10^{-6} \end{smallmatrix}\right]$ for each reactor and the separator, respectively. To reduce oscillations, the robust controller [75] is used only when the state is outside a small neighborhood of the desired equilibrium point, and a constraint of the form $V_i(x_i(t+\Delta)) \leq \delta_i$, where δ_i is a design parameter, is incorporated in the computation of the prescribed input when the state is inside that neighborhood at time t.

To demonstrate the off-line design algorithm of handling parallel and recycle streams in the safe-parking approach, we consider the two faults described in Section 5.2.2. First, we consider the fault in Q_1, with $p = 1$, to illustrate how to handle parallel streams. By following Step 2 of Algorithm 5.1, we first determine which units need to be safe-parked in the presence of the fault. At the beginning, we have $\mathcal{S} = \mathcal{J}_1 = \{1\}$ and $\mathcal{E}_1 = \varnothing$. Since $\mathcal{S} \neq \varnothing$, we pick $j = 1$ from $\mathcal{S}$ and remove 1 from $\mathcal{S}$, leading to $\mathcal{S} = \varnothing$ (see Step 2a). Because no recycle stream is detected, let $\mathcal{T} = \mathcal{I}_1 \backslash \mathcal{J}_1 = \{2, 3\}$ (see Step 2b). Since $\mathcal{T} \neq \varnothing$, we characterize $D_{1,2}$, as shown in Fig. 5.3, and remove 2 from $\mathcal{T}$, resulting

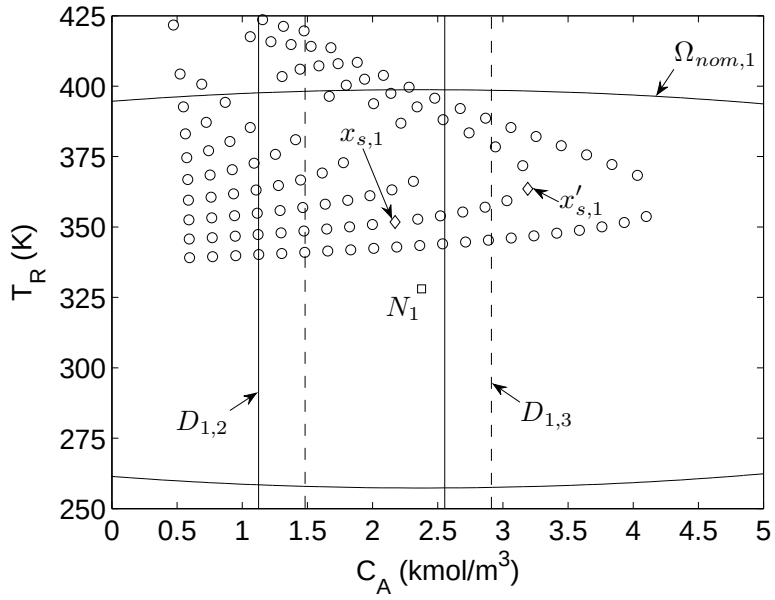

Figure 5.3: Stability region of the nominal equilibrium point for reactor-1 ($\Omega_{nom,1}$), sets $D_{1,2}$ and $D_{1,3}$, and feasible equilibrium points (marked by circles and diamonds) subject to the fault in Q_1. Since $x'_{s,1} \in \Omega_{nom,1}$, it is a valid safe-park point candidate for reactor-1 as an isolated unit. However, $x'_{s,1} \notin D_{1,2} \cap D_{1,3}$, so it does not allow continuation of nominal operation in the downstream units. In contrast, $x_{s,1} \in \Omega_{nom,1} \cap D_{1,2} \cap D_{1,3}$, so it allows continuation of nominal operation in the downstream units.

in $\mathcal{T} = \{3\}$ (see Step 2c). Because $C_1 \cap D_{1,2} \neq \varnothing$, where $C_1 = \Omega_{nom,1}$, we add 1 to $\mathcal{E}_1$ and 2 to $\mathcal{L}_1$, yielding $\mathcal{E}_1 = \{1\}$ and $\mathcal{L}_1 = \{2\}$ (see Step 2d). Then, we go back to Step 2c. Because $\mathcal{T} \neq \varnothing$, we characterize $D_{1,3}$, as shown in Fig. 5.3, and remove 3 from $\mathcal{T}$, leading to $\mathcal{T} = \varnothing$. Because $C_1 \cap D_{1,3} \neq \varnothing$, where $C_1 = \Omega_{nom,1} \cap D_{1,2}$, we have $\mathcal{E}_1$ remaining the same and $\mathcal{L}_1 = \{2, 3\}$ (see Step 2d). Next, we go back to Step 2c again. Because $\mathcal{T} = \varnothing$, we go back to Step 2a. Because $\mathcal{S} = \varnothing$, we proceed to Step 3. The evolution of different sets in Step 2 is shown in Table 5.3, where the arrow means that the corresponding set remains the same as it is in the previous step. Finally, we have $\mathcal{J}_1 = \mathcal{E}_1 = \{1\}$, $\mathcal{L}_1 = \{2, 3\}$, and $\tilde{D}_1 = D_{1,2} \cap D_{1,3}$, which means that reactor-1 needs to be safe-parked, with nominal operation in reactor-2 and reactor-3 preserved. Safe-park point candidates for reactor-1 and their associated stability regions under the reduced control action are generated in Steps 3 and 4.

In addition to the off-line design of the safe-parking framework, we implement the FDI scheme proposed in Section 5.3, which utilizes the same bounds on uncertainty and disturbances as the controller design. In particular, the following residuals (see Step 2 in

Table 5.3: Illustration of Step 2 in Algorithm 5.1 for the networked process system of Section 5.2.2.

Step	$\mathcal{S}$	$\mathcal{J}_1$	$\mathcal{E}_1$	$\mathcal{T}$	$\mathcal{L}_1$
2a	$\varnothing$	$\{1\}$	$\varnothing$		
2b	$\downarrow$	$\downarrow$	$\downarrow$	$\{2, 3\}$	
2c	$\downarrow$	$\downarrow$	$\downarrow$	$\{3\}$	
2d	$\downarrow$	$\downarrow$	$\{1\}$	$\downarrow$	$\{2\}$
2c	$\downarrow$	$\downarrow$	$\downarrow$	$\varnothing$	$\downarrow$
2d	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\{2, 3\}$
2c	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
2a	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$

Algorithm 5.2 for their definitions) are generated on-line for the three reactors: $\text{Res}_{C_{Ai,in}}$ and Res_{Q_i}, $i = 1, 2, 3$. Then, a fault is detected in the manipulated variable $C_{Ai,in}$ or Q_i if $\text{Res}_{C_{Ai,in}} = 1$ or $\text{Res}_{Q_i} = 1$. To reduce false alarms due to measurement noise, a fault is declared only if the same fault is detected for 5 consecutive times (i.e., $n_d = 5$). The noisy measurements are filtered before performing FDI and computing the prescribed input: $x_f(t_{k+1}) = 0.25x_f(t_k) + 0.75x_m(t_{k+1})$, where x_f and x_m denote the filtered state and noisy measurement, respectively.

In the simulation results, the process operates at the nominal equilibrium point initially, and the fault in Q_1 is introduced at time $t_f = 1$ hr. As shown in Fig. 5.4, the proposed FDI scheme detects the fault very quickly at time $t = 1.025$ hr and the fault is confirmed at time $t_d = 1.125$ hr (see Step 2 in Algorithm 5.2). To explain the results of FDI, the evolution of the prescribed inputs, the actual inputs, and the estimated bounds on the actual inputs to the plant for $C_{A1,in}$ and Q_1 is depicted by crosses, circles, and error bars, respectively, in Fig. 5.5. The fault is isolated via the prescribed value of Q_1 breaching the estimated lower bound on the actual input to the plant, as shown in Fig. 5.5(b). Upon the achievement of FDI, the safe-parking scheme is activated. If a temporary operating point is selected without considering the interconnected nature of the process (e.g., $x'_{s,1}$ in Fig. 5.3 is chosen), then nominal operation in reactor-2 and reactor-3 cannot be achieved in the presence of the fault, as shown in Figs. 5.6 and 5.7 (see S_1 in Table 5.2 for the corresponding steady-state values). In contrast, using the proposed approach, if the point $x_{s,1} \in \tilde{D}_1$ in Fig. 5.3 is selected as the safe-park point for reactor-1 (also satisfying the condition that at the time of FDI, the process state of reactor-1 resides within the stability region of that point; see Step 3 in Algorithm 5.2), nominal operation in reactor-2 and reactor-3 are achieved downstream, as shown in Figs. 5.8 and 5.9 (see S_2 in Table 5.2 for the corresponding steady-state values). At time $t_r = 2.5$ hr, the fault is rectified and nominal operation is smoothly resumed in

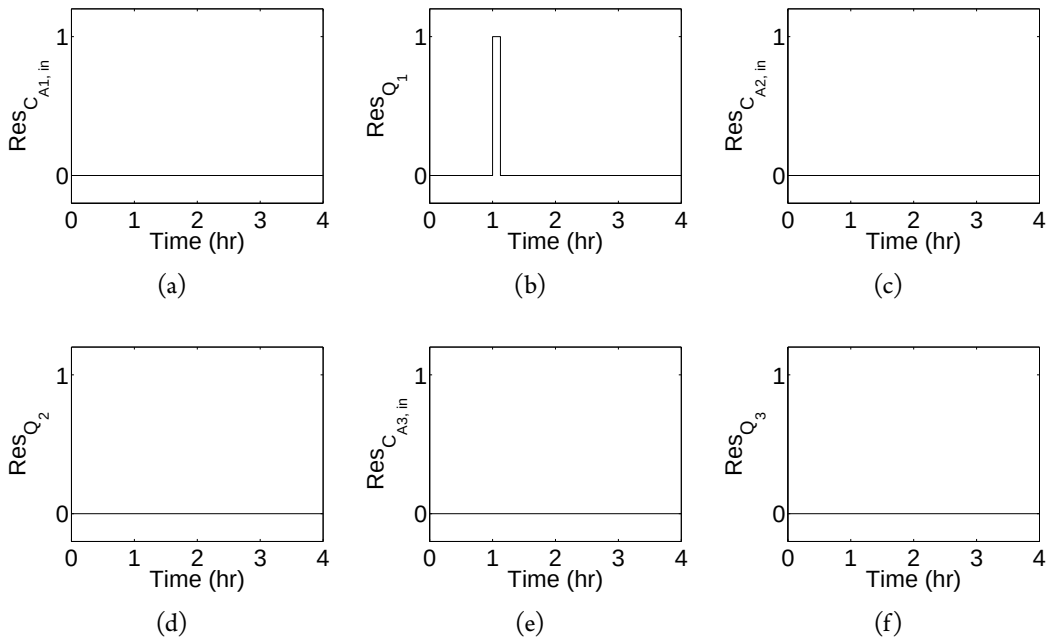

Figure 5.4: Residuals for the manipulated variables $C_{Ai,in}$ and Q_i for the three reactors, $i = 1, 2, 3$. The fault in Q_1 is first detected and isolated at time $t = 1.025$ hr and then confirmed at $t_d = 1.125$ hr.

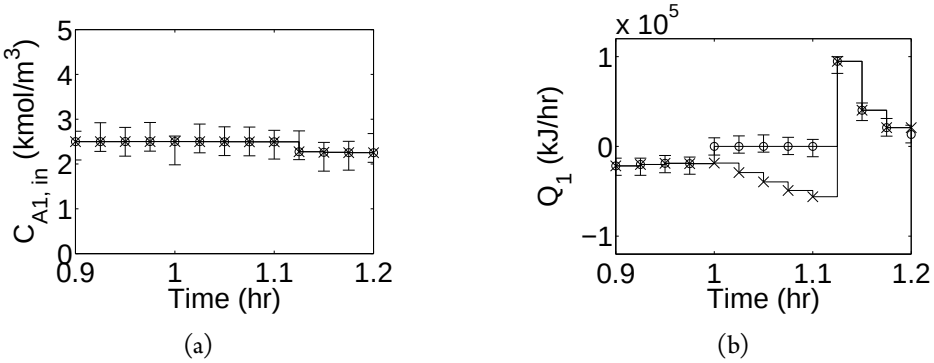

Figure 5.5: Evolution of the prescribed inputs (crosses), the actual inputs (circles), and the estimated bounds on the actual inputs (error bars) for (a) $C_{A1,in}$ and (b) Q_1 to the plant. The fault is isolated via the prescribed value of Q_1 breaching the estimated lower bound on the actual input to the plant.

reactor-1 (Step 4 in Algorithm 5.2).

Having demonstrated the case where the effect of the fault can be resisted by the downstream units, we also show a case where the plant has to be safe-parked simultaneously

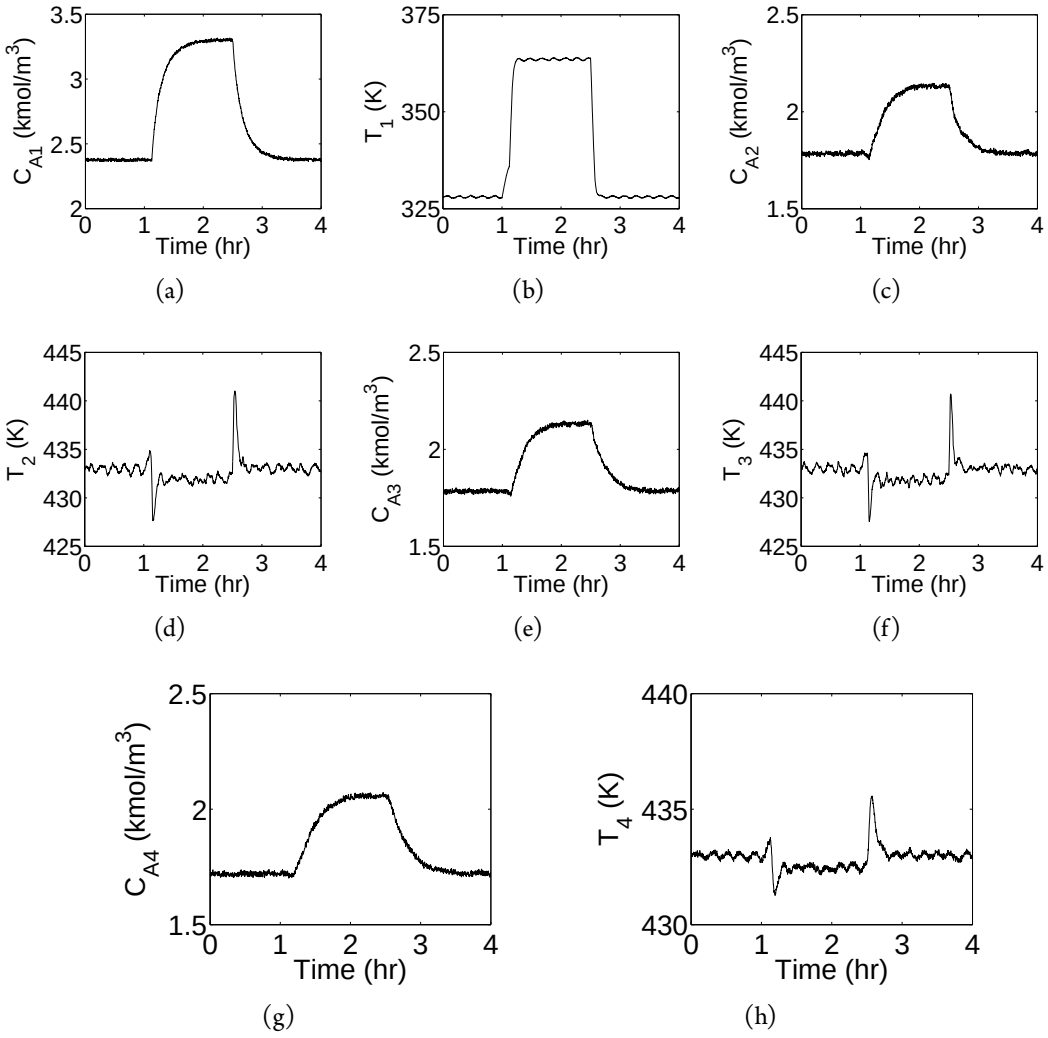

Figure 5.6: Evolution of the closed-loop state profiles for (a, b) reactor-1, (c, d) reactor-2, (e, f) reactor-3, and (g, h) the separator, where $x'_{s,1}$ is chosen as the temporary operating point for reactor-1 (which does not allow nominal operation in reactor-2, reactor-3, and the separator).

through the recycle stream to ensure safe operation. To this end, we consider the fault in $C_{A1,in}$, with $p = 2$. The fault is introduced at time $t_f = 1$ hr and repaired at time $t_r = 2.5$ hr. The temporary equilibrium points for reactor-1 in isolation subject to the fault are plotted in Fig. 5.10 by assuming nominal inlet conditions, which shows that nominal operation may be preserved in reactor-3 while safe-parking reactor-2 simultaneously. As we proceed along the network, reactor-1 is encountered again, indicating the detection of a recycle stream. Thus, we need to reexamine if nominal operation can be preserved in reactor-3. To this end, we plot the temporary equilibrium points for reactor-1 by using the model for

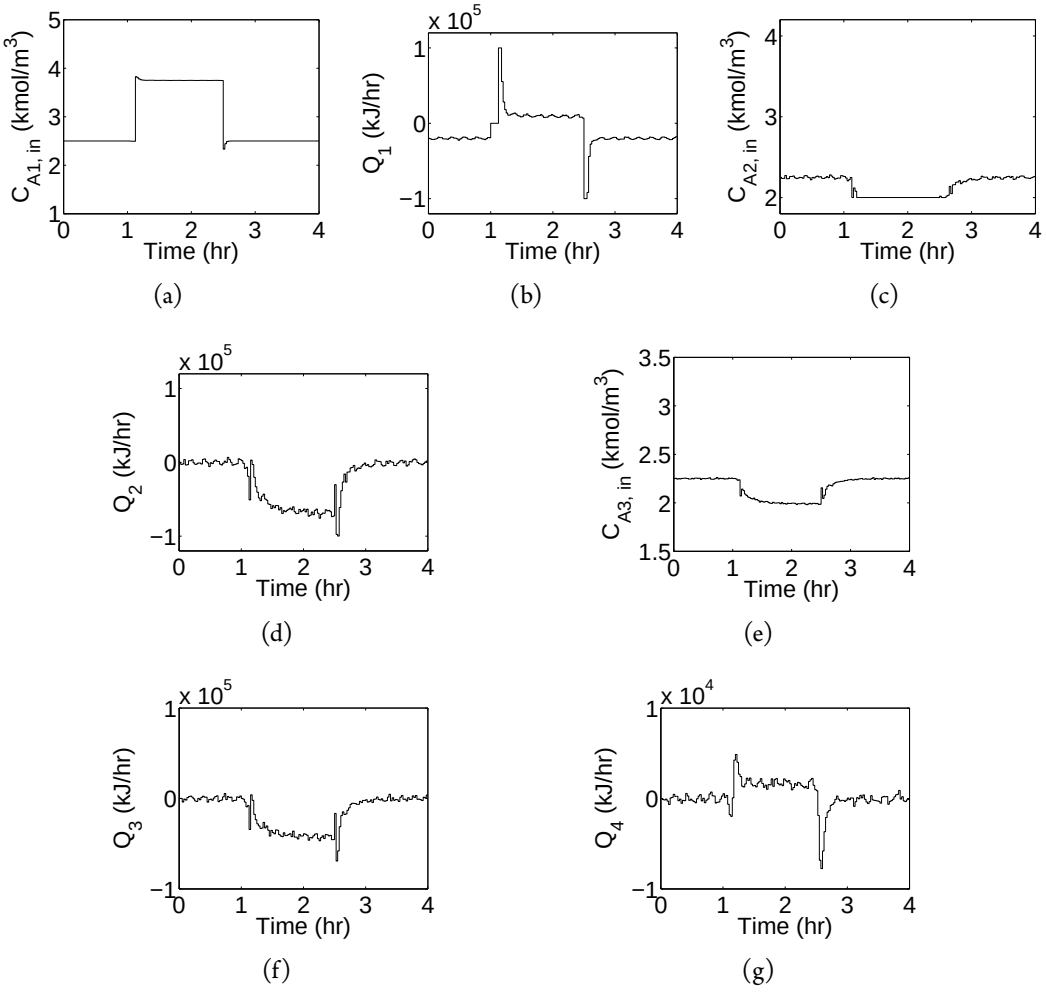

Figure 5.7: Evolution of the closed-loop input profiles for (a, b) reactor-1, (c, d) reactor-2, (e, f) reactor-3, and (g, h) the separator, where $x'_{s,1}$ is chosen as the temporary operating point for reactor-1 (which does not allow nominal operation in reactor-2, reactor-3, and the separator).

the subsystem composed of reactor-1, reactor-2, and the separator while assuming nominal conditions for the outlet stream of reactor-3, as shown in Fig. 5.11. These points are generated by discretizing the range of the available input values for reactor-1 and using nominal input values for reactor-2 and the separator. Since there exist feasible equilibrium points within $D_{1,3}$ (e.g., $x_{s,1}$ in Fig. 5.11), it is verified that nominal operation can be preserved in reactor-3. Finally, we have $\mathcal{J}_2 = \{1, 2, 4\}$, $\mathcal{E}_2 = \{1\}$, and $\mathcal{L}_1 = \{3\}$. Therefore, reactor-1, reactor-2, and the separator have to be safe-parked simultaneously, with nominal operation in reactor-3 preserved (see S_3 in Table 5.2 for the corresponding steady-state values). As shown in Fig. 5.12, the proposed FDI scheme detects and isolates the fault again very quickly at time $t = 1.025$ hr and the fault is confirmed at time $t_d = 1.125$

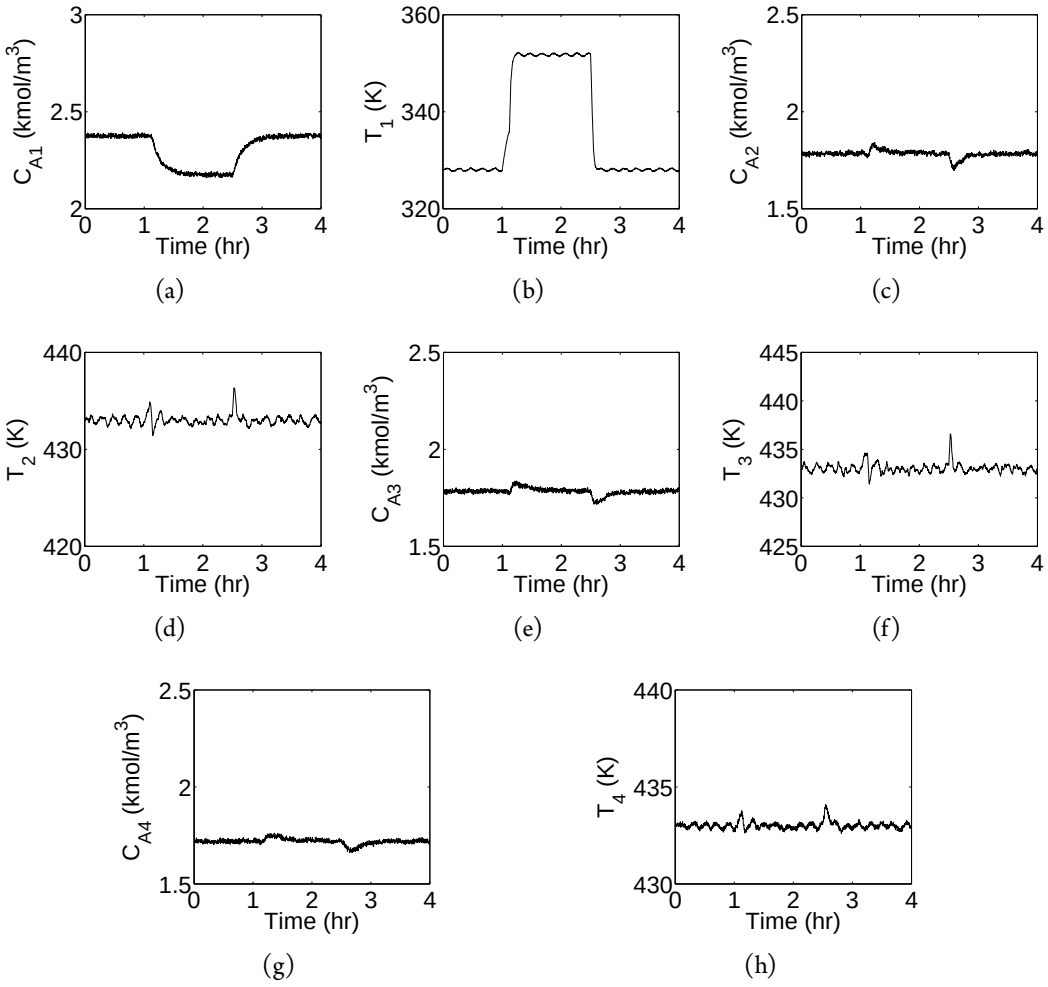

Figure 5.8: Evolution of the closed-loop state profiles for (a, b) reactor-1, (c, d) reactor-2, (e, f) reactor-3, and (g, h) the separator, where $x_{s,1}$ is chosen as the safe-park point for reactor-1 (which allows nominal operation in reactor-2, reactor-3, and the separator).

hr. Subsequently, reactor-1, reactor-2, and the separator are safe-parked, with reactor-3 continuing nominal operation even during fault rectification and the entire plant resuming nominal operation upon fault rectification. The evolution of the state and input profiles are depicted in Figs. 5.13 and 5.14, respectively.

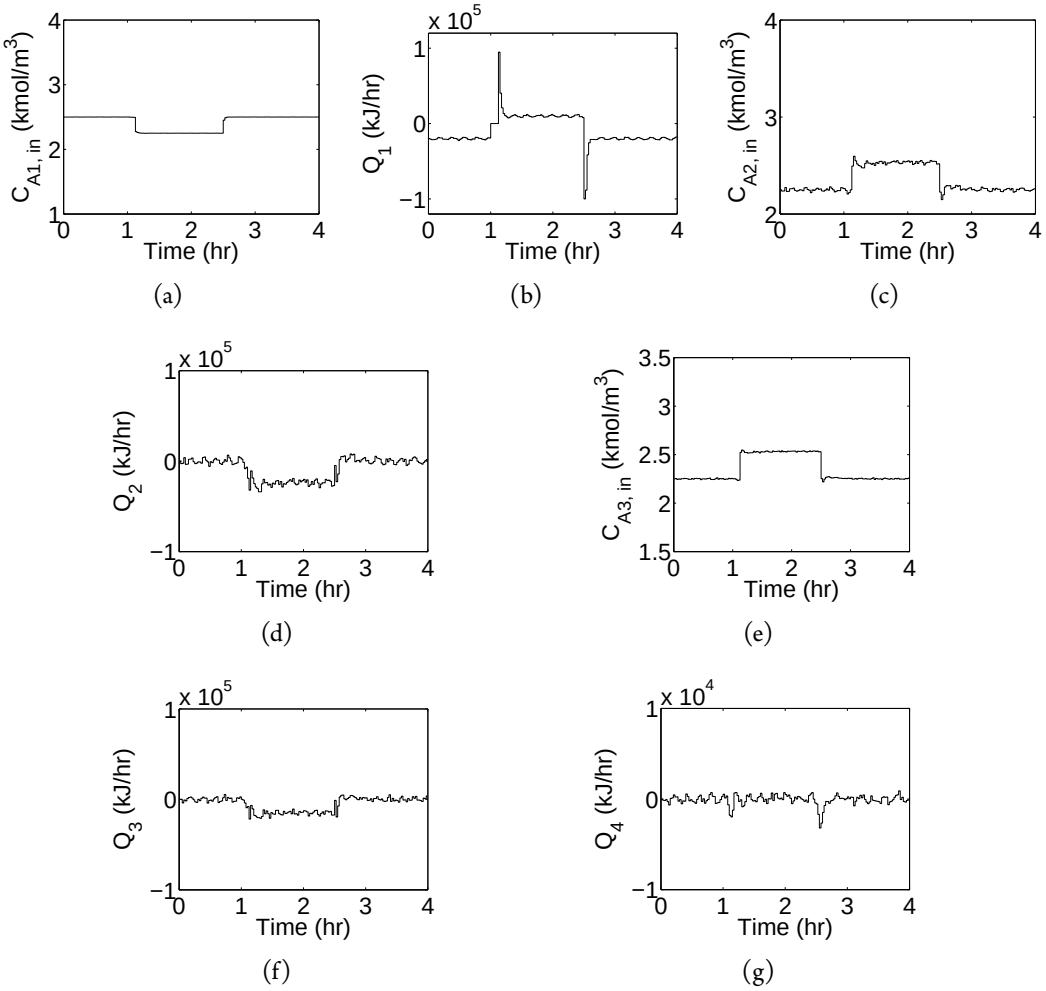

Figure 5.9: Evolution of the closed-loop input profiles for (a, b) reactor-1, (c, d) reactor-2, (e, f) reactor-3, and (g, h) the separator, where $x_{s,1}$ is chosen as the safe-park point for reactor-1 (which allows nominal operation in reactor-2, reactor-3, and the separator).

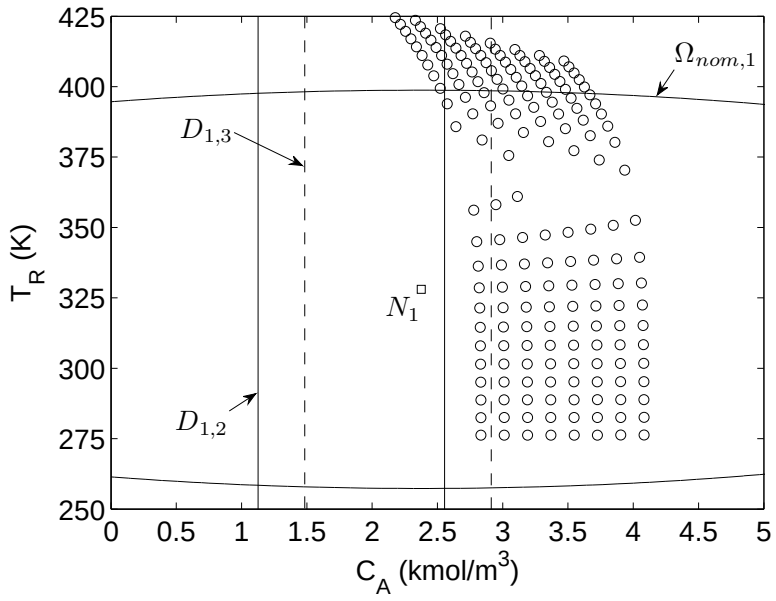

Figure 5.10: Stability region of the nominal equilibrium point for reactor-1 ($\Omega_{nom,1}$), sets $D_{1,2}$ and $D_{1,3}$, and feasible equilibrium points (marked by circles) subject to the fault in $C_{A1,in}$ for reactor-1 in isolation. None of the safe-park point candidates resides within $\Omega_{nom,1} \cap D_{1,2} \cap D_{1,3}$.

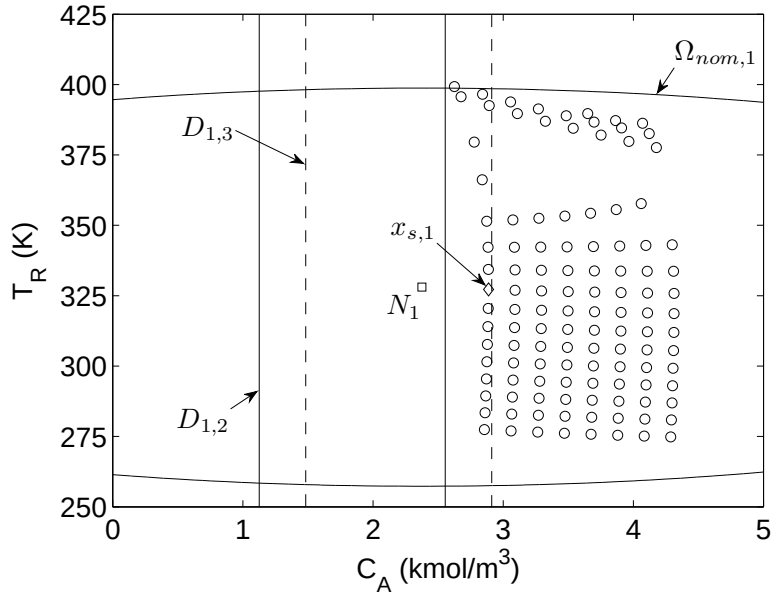

Figure 5.11: Stability region of the nominal equilibrium point for reactor-1 ($\Omega_{nom,1}$), sets $D_{1,2}$ and $D_{1,3}$, and feasible equilibrium points (marked by circles and the diamond) subject to the fault in $C_{A1,in}$ for reactor-1 in the subsystem. Since $x_{s,1} \in D_{1,3}$ (also in $\Omega_{nom,1}$), it allows continuation of nominal operation in reactor-3.

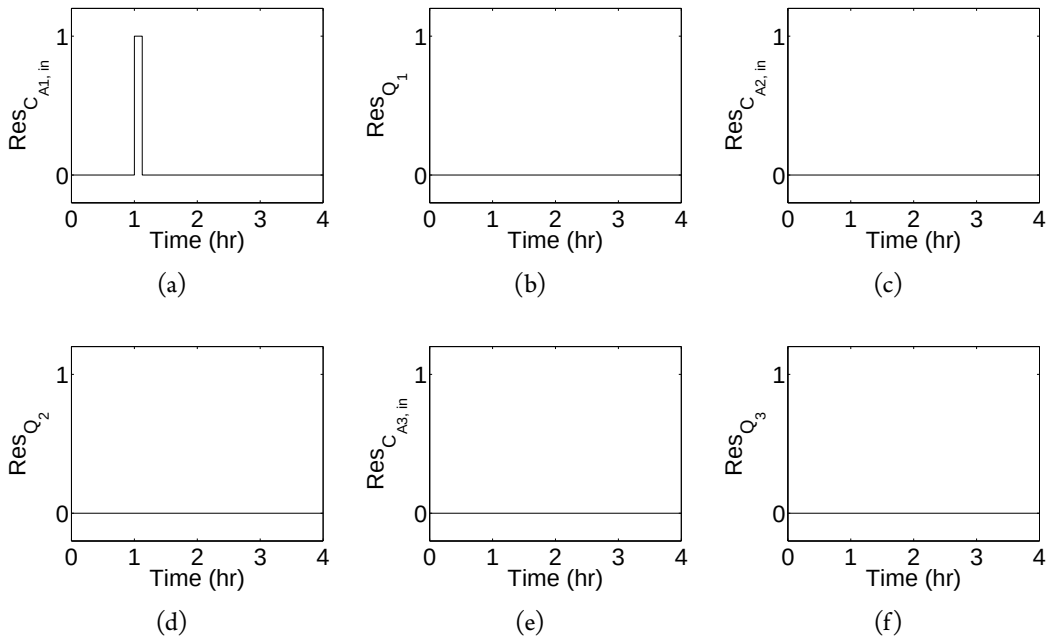

Figure 5.12: Residuals for the manipulated variables $C_{Ai,in}$ and Q_i for the three reactors, $i = 1$, 2, 3. The fault in $C_{A1,in}$ is first detected and isolated at time $t = 1.025$ hr and then confirmed at $t_d = 1.125$ hr.

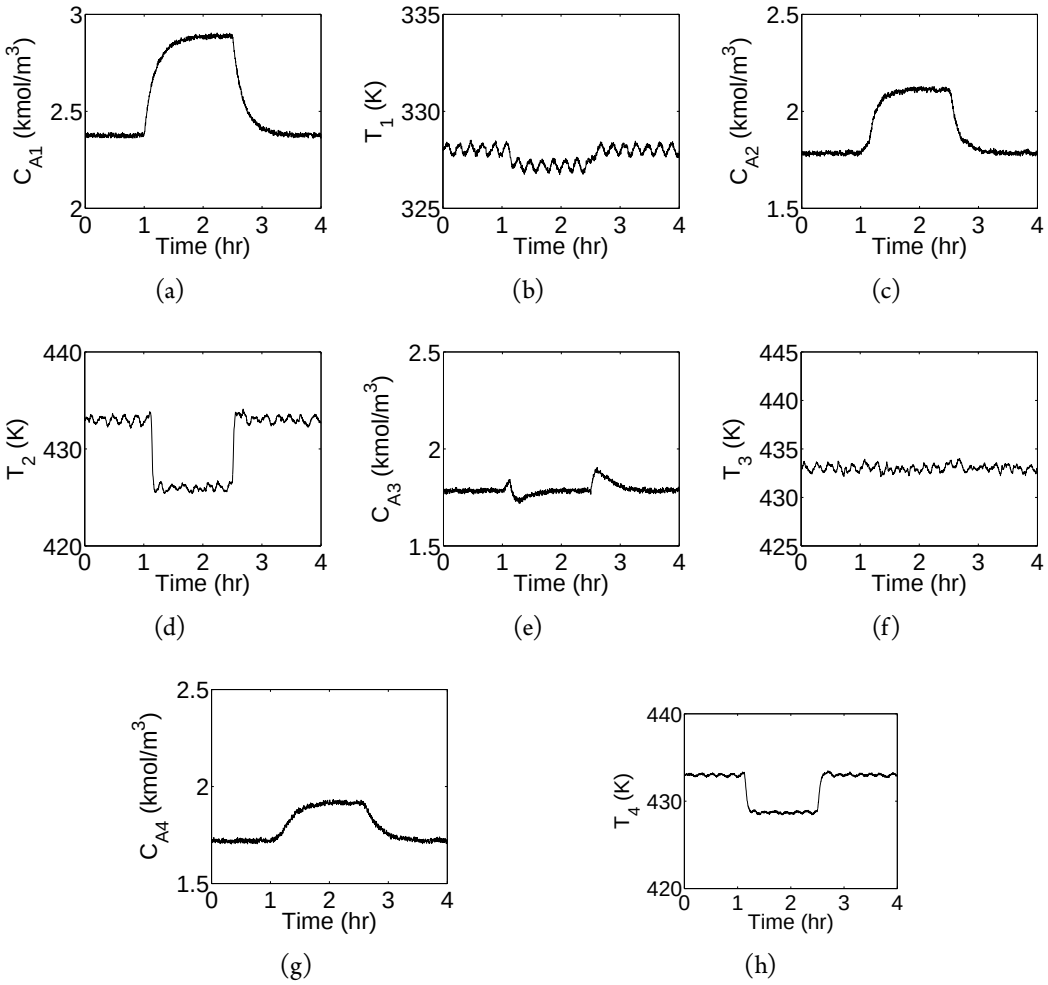

Figure 5.13: Evolution of the closed-loop state profiles for (a, b) reactor-1, (c, d) reactor-2, (e, f) reactor-3, and (g, h) the separator, where simultaneous safe-parking is implemented for reactor-1, reactor-2, and the separator.

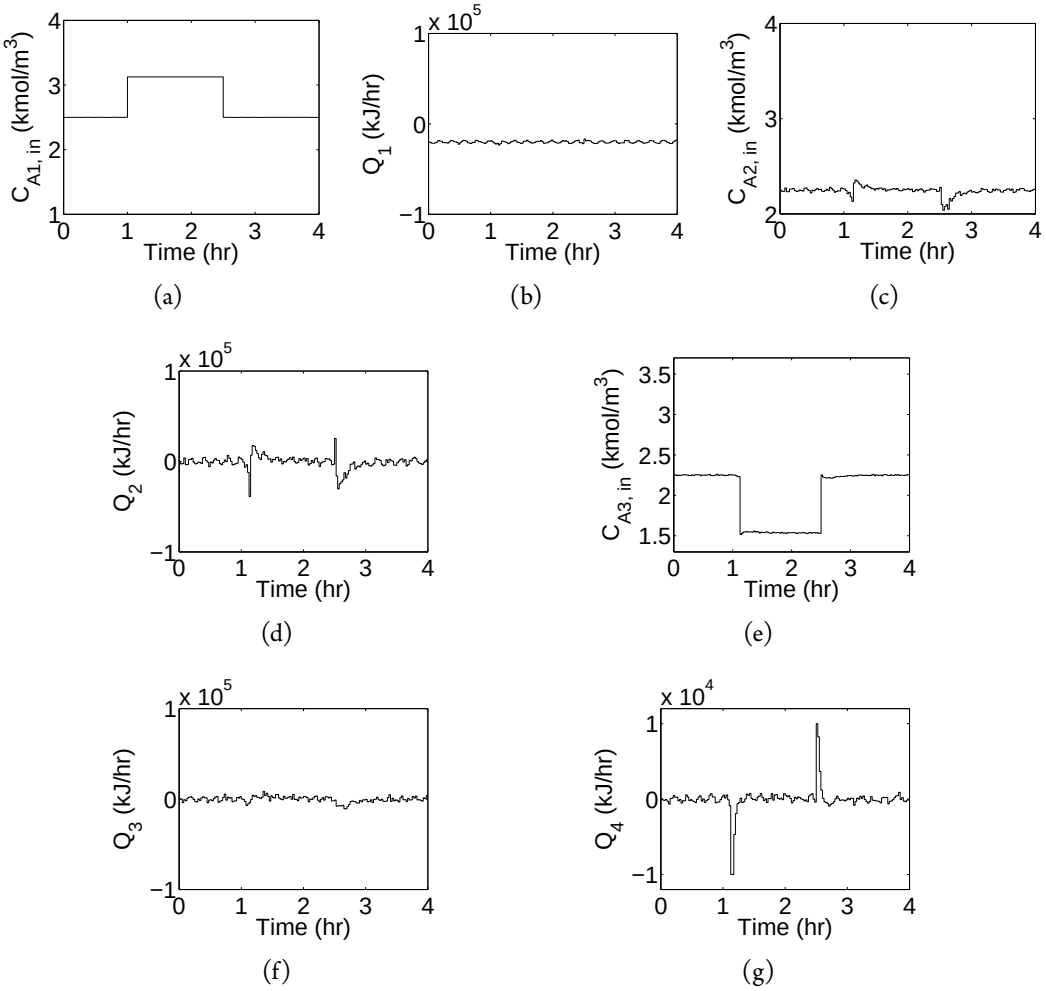

Figure 5.14: Evolution of the closed-loop input profiles for (a, b) reactor-1, (c, d) reactor-2, (e, f) reactor-3, and (g, h) the separator, where simultaneous safe-parking is implemented for reactor-1, reactor-2, and the separator.

5.6 Conclusions

This chapter considered the problem of FDI and fault-handling for networked process systems subject to actuator faults. It was assumed that the failed actuator reverts to its fail-safe position and precludes the possibility of nominal operation in the affected unit. A robust FDI design was first presented, where relations between the prescribed inputs and state measurements in the absence of faults are constructed with the consideration of uncertainty. A fault is detected and isolated when the corresponding relation is violated. An algorithm was then developed to determine the units that need to be safe-parked during the fault repair period and generate possible safe-park points for the affected units. The implementation of the safe-parking techniques is triggered by the isolation of a fault, which can localize the effect of the fault in a subsystem of the networked plant. The efficacy of the integrated FDI and safe-parking framework was demonstrated on a chemical process example comprising three reactors and a separator.

Chapter 6

Integrated Fault Diagnosis and Safe-Parking to Handle Frozen Actuators in Nonlinear Process Systems[1]

6.1 Introduction

The problem of FTC has been studied extensively using the robust/reliable control [62, 63] or control reconfiguration approaches [27, 64]. The robust/reliable control approach considers the case where the residual control ability of the active control actuators is able to preserve nominal operation. These passive FTC methods do not require the use of FDI in the fault-handling mechanism design. The control reconfiguration approach considers the case where the active control configuration is not able to preserve nominal operation under faulty conditions. To maintain the process at the nominal operating point, an appropriate backup control configuration is activated, where the failed actuator is not used. In this approach, it is assumed that the faulty actuator can be "removed" from the control loop and its control action is set to its "nominal" value. In addition, the safe-parking approach presented in Chapters 4 and 5 studies the problem of handling actuator faults in

[1] The results in this chapter have been published in:

a. M. Du, J. Nease, and P. Mhaskar. An integrated fault diagnosis and safe-parking framework for fault-tolerant control of nonlinear systems. *Int. J. Rob. & Non. Contr.*, 22:105–122, 2012.

b. M. Du, R. Gandhi, and P. Mhaskar. Fault detection and isolation and safe-parking of networked systems. In *Proceedings of the 2011 American Control Conference*, pages 3146–3151, San Francisco, CA, 2011.

the absence of sufficient residual control ability or the availability of backup control configurations. Instead of requiring the failed actuator be "removed" from the control loop, it considers the case where the failed actuator reverts to a fail-safe position, which is a built-in actuator position to prevent the occurrence of hazardous situations. The knowledge about the failed actuator position is known in advance and used in the safe-parking design.

Since the control reconfiguration and safe-parking designs in [27, 62–64, 74–76, 85, 86] only require the information about the location of the fault, relatively less attention has been paid to the problem of identifying the magnitudes of faults and using this information in the fault-handling mechanism design. As mentioned in Chapter 1, another case of a complete actuator failure is that the failed actuator seizes at an arbitrary position. For example, it is frozen at the position before the fault takes place. In this case, it is highly possible that the nominal equilibrium point is no longer an equilibrium point in the presence of faults. Therefore, the FTC methods in [62, 64] may not remain applicable. Since the safe-parking designs in [74–76, 85, 86] are based on fail-safe positions, they do not remain directly applicable to the case where the failed actuator is frozen at an arbitrary position. To generalize the idea of safe-parking, a fault detection and diagnosis (FDD) mechanism is required to provide an estimate of the failed actuator position. Furthermore, the unavailability of *a prior* knowledge about the the failed actuator position should be accounted for in the off-line design of the safe-park point candidates and the on-line decision of a safe-park point.

Motivated by the above considerations, this chapter considers the problem of designing an integrated fault diagnosis and safe-parking framework to deal with actuator faults in nonlinear process systems. To this end, a model-based fault diagnosis design is first proposed, which can not only identify the failed actuator, but also estimate the fault magnitude. The fault information is obtained by estimating the outputs of the actuators and comparing them with the corresponding prescribed control inputs. This methodology is first developed under state feedback control and then generalized to deal with state estimation errors. In the safe-parking design, possible safe-park points are generated for a series of design values of the failed actuator position. After a fault is diagnosed, the estimate of the failed actuator position is used to choose a safe-park point. The discrepancy between the actual value of the failed actuator position and the corresponding design value is handled through the robustness of the control design. The efficacy of the integrated fault diagnosis and safe-parking framework is demonstrated through a chemical reactor example.

The remainder of this chapter is organized as follows. In Section 6.2, the class of systems considered and a control design used to illustrate the safe-parking framework are

presented. The model-based fault diagnosis design is proposed in Section 6.3. The safe-parking design is developed in Section 6.4. The simulation results are presented in Section 6.5. Finally, Section 6.6 presents some concluding remarks.

6.2 Preliminaries

In this section, we present the system description and a robust control design, which will be used to illustrate the safe-parking framework in Section 6.5.

6.2.1 System Description

Consider a nonlinear system subject to actuator faults with the following state-space description:

$$\begin{aligned} &\dot{x} = f(x,\theta(t)) + G(x)[u(t)+\tilde{u}(t)] \\ &u(t) \in \mathcal{U}, \theta(t) \in \Theta \\ &u(t)+\tilde{u}(t) = u(t_k)+\tilde{u}(t_k) \in \mathcal{U} \text{ for all } t \in [t_k, t_{k+1}), k = 0, \ldots, \infty \end{aligned} \tag{6.1}$$

where $x = [x_1, \ldots, x_n]^{\mathrm{T}} \in \mathbb{R}^n$ is the vector of state variables, $u = [u_1, \ldots, u_m]^{\mathrm{T}} \in \mathbb{R}^m$ is the vector of prescribed control inputs given by the control law and $\tilde{u} = [\tilde{u}_1, \ldots, \tilde{u}_m]^{\mathrm{T}} \in \mathbb{R}^m$ is the unknown fault vector for the actuators, with the actual control input $u + \tilde{u}$ implemented to the plant taking values in a nonempty compact convex set $\mathcal{U} := \{u \in \mathbb{R}^m : u_{\min} \leq u \leq u_{\max}\}$ that contains 0, where $u_{\min} = [u_{1,\min}, \ldots, u_{m,\min}]^{\mathrm{T}} \in \mathbb{R}^m$ and $u_{\max} = [u_{1,\max}, \ldots, u_{m,\max}]^{\mathrm{T}} \in \mathbb{R}^m$ denote the lower and upper bounds (constraints) on the vector of manipulated variables, respectively, and $\theta = [\theta_1, \ldots, \theta_q]^{\mathrm{T}} \in \mathbb{R}^q$ is the vector of (possibly time-varying) uncertain variables taking values in a nonempty compact convex set $\Theta := \{\theta \in \mathbb{R}^q : \theta_{\min} \leq \theta \leq \theta_{\max}\}$ that contains 0, where $\theta_{\min} = [\theta_{1,\min}, \ldots, \theta_{q,\min}]^{\mathrm{T}} \in \mathbb{R}^q$ and $\theta_{\max} = [\theta_{1,\max}, \ldots, \theta_{q,\max}]^{\mathrm{T}} \in \mathbb{R}^q$ denote the lower and upper bounds on the vector of uncertain variables, respectively. It is assumed that the functions $f(x,\theta) = [f_i(x,\theta)]_{n\times 1}$ and $G(x) = [g_{ij}(x)]_{n\times m}$ are locally Lipschitz in their arguments, and $f(x,\theta)$ is differentiable with respect to θ ($i = 1, \ldots, n$; $j = 1, \ldots, m$). The origin is an equilibrium point of the nominal system (the system of Eq. (6.1) with $\tilde{u}(t) \equiv 0$ and $\theta(t) \equiv 0$) for $u = 0$, i.e., $f(0,0) = 0$. The control input is prescribed at discrete times $t_k := k\Delta$, $k = 0, \ldots, \infty$, where Δ denotes the period during which the control action is kept constant. The faults considered are such that an actuator seizes at an

arbitrary position. It is assumed that the corrupted input to the plant is constant during each time interval; that is, $u(t) + \tilde{u}(t) = u(t_k) + \tilde{u}(t_k)$ for all $t \in [t_k, t_{k+1})$. Note that $-u_{\min}$ (or $-\theta_{\min}$) does not have to be equal to $u_{\max}$ (or $\theta_{\max}$), and we have that $\|u\| \leq u_b$ and $\|\theta\| \leq \theta_b$, where $u_b = \|[\max\{-u_{1,\min}, u_{1,\max}\}, \ldots, \max\{-u_{m,\min}, u_{m,\max}\}]^{\mathrm{T}}\|$ and $\theta_b = \|[\max\{-\theta_{1,\min}, \theta_{1,\max}\}, \ldots, \max\{-\theta_{q,\min}, \theta_{q,\max}\}]^{\mathrm{T}}\|$.

6.2.2 Lyapunov-Based Predictive Control

To illustrate the safe-parking framework for FTC, the Lyapunov-based predictive controller developed in [75] is adapted under Assumption 6.1 below and used as an example of a robust control design with a well characterized stability region.

Assumption 6.1. For the system of Eq. (6.1), $f_i(x, \theta)$, $i = 1, \ldots, n$, is monotonic with respect to θ_j, $j = 1, \ldots, q$, for any $x \in \mathbb{R}^n$ and $\theta_l \in [\theta_{l,\min}, \theta_{l,\max}]$, $l = 1, \ldots, q$ and $l \neq j$.

Remark 6.1. In many practical process systems, the form of $f(x, \theta)$ is known and the uncertain variables affect $f(x, \theta)$ monotonically, as required in Assumption 6.1. For example, in the Arrhenius law of reaction rates, the parametric uncertainty includes errors in the pre-exponential constant and the activation energy. The reaction rate is monotonically increasing with respect to the pre-exponential constant, while it is monotonically decreasing with respect to the activation energy. Other uncertainty includes the enthalpy of reaction and the heat transfer coefficient. In addition to the parametric uncertainty, θ also models the unknown disturbances entering the system. Typical disturbances include errors in the temperature and concentration of a feed stream, or the temperature of a cooling stream, which also affect the value of $f(x, \theta)$ monotonically. While we work with Assumption 6.1 to simplify the presentation, it should be noted that a more general assumption can be stated as follows: there exist known functions $f_l(x)$ and $f_u(x)$ such that $f_l(x) \leq f(x, \theta) \leq f_u(x)$ for all $\theta \in \Theta$.

Consider the system of Eq. (6.1) under fault-free conditions, for which a CLF $V(x)$ exists and Assumption 6.1 holds. Let Π denote a set of states where $\dot{V}(x(t))$ can be made negative by using the allowable values of the constrained input:

$$\Pi = \left\{ x \in \mathbb{R}^n : \sup_{\theta \in \Theta} L_f V(x, \theta) + \inf_{u \in \mathcal{U}} L_G V(x) u \leq -\varepsilon V(x) \right\} \tag{6.2}$$

where $L_G V(x) = [L_{g_1} V(x), \ldots, L_{g_m} V(x)]$, with g_i being the ith column of G, and ε is a positive real number. It is assumed that $L_f V(x, \theta)$ and $L_G V(x)$ are locally Lipschitz. To esti-

mate the upper bound on $L_f V(x,\theta)$, let $\theta_{i,l} = [\theta_{i,1,l}, \ldots, \theta_{i,q,l}]$ and $\theta_{i,u} = [\theta_{i,1,u}, \ldots, \theta_{i,q,u}]$, $i = 1, \ldots, n$, where $\theta_{i,j,l} = \begin{cases} \theta_{j,\max}, & \text{if } \frac{df_i}{d\theta_j} \leq 0 \\ \theta_{j,\min}, & \text{if } \frac{df_i}{d\theta_j} > 0 \end{cases}$ and $\theta_{i,j,u} = \begin{cases} \theta_{j,\min}, & \text{if } \frac{df_i}{d\theta_j} \leq 0 \\ \theta_{j,\max}, & \text{if } \frac{df_i}{d\theta_j} > 0 \end{cases}$, $j = 1, \ldots, q$. Note that $\theta_{i,l}$ and $\theta_{i,u}$ are the instances of θ that make $f_i(x,\theta)$ take its minimum and maximum values for given x, respectively. Let $\tilde{\theta}_i = \begin{cases} \theta_{i,l}, & \frac{\partial V}{\partial x_i} \leq 0 \\ \theta_{i,u}, & \frac{\partial V}{\partial x_i} > 0 \end{cases}$, $i = 1, \ldots, n$. It follows that $\sum_{i=1}^{n} \frac{\partial V}{\partial x_i} f_i(x, \tilde{\theta}_i)$ is an estimate of the upper bound on $L_f V(x,\theta)$. Note that $\inf_{u \in \mathcal{U}} L_G V(x) u$ can be computed in a similar way. The robust controller of [75] possesses a stability region, an estimate of which is given by:

$$\{x \in \Pi' : V(x) \leq c\} \tag{6.3}$$

where Π' is an estimate of Π by replacing $\sup_{\theta \in \Theta} L_f V(x,\theta)$ with $\sum_{i=1}^{n} \frac{\partial V}{\partial x_i} f_i(x, \tilde{\theta}_i)$ and c is a positive (preferably the largest possible) constant.

The Lyapunov-based predictive controller adapted from [75] takes the following form:

$$u^*(\cdot) = \operatorname{argmin}\{J(x,t,u(\cdot)) | u(\cdot) \in S\} \tag{6.4a}$$

$$\text{s.t.} \quad \dot{x} = f(x,0) + G(x)u \tag{6.4b}$$

$$L_G V(x(t)) u(t) \leq -\sum_{i=1}^{n} \frac{\partial V}{\partial x_i} f_i(x, \tilde{\theta}_i) - \varepsilon V(x(t)) \tag{6.4c}$$

$$x(\tau) \in \Pi' \text{ for all } \tau \in [t, t+\Delta) \tag{6.4d}$$

where $S = S(t,T)$ is a family of piecewise continuous functions (functions continuous from the right), with T denoting the control horizon, mapping $[t, t+T)$ into $\mathcal{U}$. A control $u(\cdot)$ in S is characterized by the sequence $\{u(t_k)\}$ and satisfies $u(\tau) = u(t_k)$ for all $\tau \in [t_k, t_k + \Delta)$. The objective function is given by

$$J(x,t,u(\cdot)) = \int_t^{t+T} \left[\|x^u(s;x,t)\|_{Q_w}^2 + \|u(s)\|_{R_w}^2 \right] ds \tag{6.5}$$

where Q_w is a positive semi-definite symmetric matrix, R_w is a strictly positive definite symmetric matrix, and $x^u(s;x,t)$ denotes the solution of Eq. (6.4b), due to control $u(\cdot)$, with the initial state x at time t. In accordance with the receding horizon implementation, the minimizing control $u^*(\cdot)$ is then applied to the system over $[t, t+\Delta)$ and the same procedure is repeated at the next instant.

The stability property of the control law of Eq. (6.4) can be formulated as follows: given any positive real number d, there exists a positive real number Δ^* such that if $\Delta \in (0, \Delta^*]$ and $x(0) \in \Omega$, then $x(t) \in \Omega$ for all $t \geq 0$ and $\limsup_{t\to\infty} \|x(t)\| \leq d$ (see [75] for further details on the control design). Finally, note that while the control law of Eq. (6.4) is used as an example of a control design for illustration, the proposed results hold under any control law (which we refer to as $RC(x)$) satisfying Assumption 6.2 below.

Assumption 6.2. For the system of Eq. (6.1) under fault-free conditions, there exist a robust control law $RC(x)$ and a set $\Omega \subseteq \mathbb{R}^n$ such that given any positive real number d, there exist positive real numbers Δ^* and T_f such that if $\Delta \in (0, \Delta^*]$ and $x(0) \in \Omega$, then $x(t) \in \Omega$ for all $t \geq 0$ and $\|x(t)\| \leq d$ for all $t \geq T_f$.

6.3 Fault Detection and Diagnosis Structure

In this section, we first propose a fault diagnosis design under state feedback control in Section 6.3.1, and then generalize it to handle state estimation errors in Section 6.3.2.

6.3.1 Fault Diagnosis under State Feedback Control

In this section, under the assumption of full state feedback, we design an FDI scheme using constant thresholds and then for a special case, devise an FDD scheme using time-varying thresholds. With the assumption that $m \leq n$, the system of Eq. (6.1) can be decomposed into two coupled subsystems: what we denote as a diagnosable subsystem and the remainder of the original system, with states denoted by $x_d \in \mathbb{R}^m$ and $x_{\bar{d}} \in \mathbb{R}^{n-m}$, respectively. Accordingly, we have $f(x,\theta) = [f_d(x,\theta)^{\mathrm{T}}, f_{\bar{d}}(x,\theta)^{\mathrm{T}}]^{\mathrm{T}}$ and $G(x) = [G_d(x)^{\mathrm{T}}, G_{\bar{d}}(x)^{\mathrm{T}}]^{\mathrm{T}}$. The system of Eq. (6.1) can then be written as follows:

$$\dot{x}_d = f_d(x,\theta) + G_d(x)[u(t) + \tilde{u}(t)] \tag{6.6a}$$

$$\dot{x}_{\bar{d}} = f_{\bar{d}}(x,\theta) + G_{\bar{d}}(x)[u(t) + \tilde{u}(t)] \tag{6.6b}$$

The key idea of the proposed methodology is to estimate the outputs of the actuators by using the system model and state measurements, and then compare them with the corresponding prescribed control inputs to construct input-based residuals. To this end, consider the time interval $[t_k, t_{k+1})$, with t_{k+1} being the current time. Integrating both sides of

Eq. (6.6a) over $[t_k, t_{k+1})$ gives the following equation:

$$\begin{aligned} x_d(t_{k+1}) &= x_d(t_k) + \int_{t_k}^{t_{k+1}} \{f_d(x,\theta) + G_d(x)[u(t) + \tilde{u}(t)]\}dt \\ &= x_d(t_k) + F_{d,k} + G_{d,k}[u(t_k) + \tilde{u}(t_k)] \end{aligned} \tag{6.7}$$

where $F_{d,k} = \int_{t_k}^{t_{k+1}} f_d(x,\theta)dt$ and $G_{d,k} = \int_{t_k}^{t_{k+1}} G_d(x)dt$. Let $x_{d,i}, f_{d,i}, F_{d,i,k}$, and $G_{d,i,k}$ denote the ith element or row of $x_d, f_d, F_{d,k}$, and $G_{d,k}$, respectively, for $i = 1, \ldots, m$. We say that the subsystem of Eq. (6.6a) is diagnosable if it satisfies Assumption 6.3 below.

Assumption 6.3. For the system of Eq. (6.1), $m \leq n$ and $G_{d,k}$ is invertible for $k = 0, \ldots, \infty$.

Remark 6.2. To illustrate the idea behind Assumption 6.3, consider a scalar system described by $\dot{x} = x + u_1 + 2u_2$, where $x, u_1, u_2 \in \mathbb{R}$. For this system, it is impossible to differentiate between faults in u_1 and u_2 because the number of state variables is eclipsed by that of the input variables (i.e., $m > n$). Alternatively, it is possible that inputs affect states in the same manner through different channels. For example, consider the system described by $\dot{x} = x + \left[\begin{smallmatrix} 1 & 1 \\ 2 & 2 \end{smallmatrix}\right] u$, where $x, u \in \mathbb{R}^2$. For this case, the definition of a new variable $v = u_1 + u_2$ leads to an equivalent system of the form $\dot{x} = x + [1,2]^{\mathrm{T}} v$. Although the number of state variables is equal to that of the input variables in the original system, any fault in u_1 or u_2 can be seen as a fault in v, thereby impeding fault isolation. A simple example of a diagnosable system is given by $\dot{x} = x + \left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right] u$, where $x, u \in \mathbb{R}^2$. In this example, u_2 affects x_1 more than u_1, and u_1 affects x_2 more than u_2, thereby satisfying the condition that the inputs affect the state dynamics uniquely through different channels.

Remark 6.3. In [27], the isolation of faults relies on the assumption that there exists a state variable such that its evolution is directly and uniquely affected by the potential fault. Specifically, it requires that for every input u_j, $j = 1, \ldots, m$, there exist a state x_i, $i \in \{1, \ldots, n\}$ such that with x_i as an output, the relative degree of x_i with respect to u_j and only with respect to u_j is equal to 1. In other words, $g_{i,j}(x) \neq 0$ for all $x \in \mathbb{R}^n$ and $g_{i,l}(x) \equiv 0$ for $l = 1, \ldots, m$ and $l \neq j$. In this case, $G_d(x)$ is a diagonal matrix with non-zero elements on its diagonal. Therefore, $G_{d,k}$ is invertible. Assumption 6.3, however, only requires that $G_{d,k}$ be invertible, and $G_d(x)$ could be a non-diagonal matrix.

Let $[G_{d,k}^{-1}]_i$ denote the ith row of $G_{d,k}^{-1}$ and $[G_{d,k}^{-1}]_{ij}$ denote the jth element of $[G_{d,k}^{-1}]_i$. It follows from Eq. (6.7) that

$$u_i(t_k) + \tilde{u}_i(t_k) = [G_{d,k}^{-1}]_i [x_d(t_{k+1}) - x_d(t_k) - F_{d,k}] \tag{6.8}$$

For $i = 1, \ldots, m$, define the residuals as

$$r_{i,k} = \left| [G_{d,k}^{-1}]_i [x_d(t_{k+1}) - x_d(t_k) - \bar{F}_{d,k}] - u_i(t_k) \right| \tag{6.9}$$

where $\bar{F}_{d,k} = \int_{t_k}^{t_{k+1}} f_d(x, 0)dt$. Note that $[G_{d,k}^{-1}]_i [x_d(t_{k+1}) - x_d(t_k) - \bar{F}_{d,k}]$ is the estimate of the actual input to the plant by using the nominal system model. Substituting $u_i(t_k)$ in Eq. (6.8) into Eq. (6.9) gives $r_{i,k} = \left| [G_{d,k}^{-1}]_i (F_{d,k} - \bar{F}_{d,k}) + \tilde{u}_i(t_k) \right|$. The FDI scheme using constant thresholds is formalized in Theorem 6.1 below.

Theorem 6.1. *Consider the system of Eq. (6.1), for which Assumption 6.3 holds. Assume that* $\| [G_{d,k}^{-1}]_i^T \| \leq K_{g,i}$ *for* $k = 0, \ldots, \infty$, *where* $K_{g,i}$ *is a positive real number. Then, there exists* $\delta_i > 0$ *such that if* $r_{i,k} > \delta_i$, *then* $\tilde{u}_i(t_k) \neq 0$.

Proof. Since $f_d(x, \theta)$ is locally Lipschitz in θ, there exists $L_f > 0$ such that

$$\| f_d(x, \theta) - f_d(x, 0) \| \leq L_f \theta_b \tag{6.10}$$

If $\tilde{u}_i(t_k) = 0$, it follows that

$$r_{i,k} = \left| [G_{d,k}^{-1}]_i (F_{d,k} - \bar{F}_{d,k}) \right| = \left| [G_{d,k}^{-1}]_i \int_{t_k}^{t_{k+1}} [f_d(x, \theta) - f_d(x, 0)] dt \right| \leq K_{g,i} L_f \theta_b \Delta \tag{6.11}$$

It means that for $\delta_i = K_{g,i} L_f \theta_b \Delta$, if $\tilde{u}_i(t_k) = 0$, then $r_{i,k} \leq \delta_i$. Therefore, $r_{i,k} > \delta_i$ implies that $\tilde{u}_i(t_k) \neq 0$. This concludes the proof of Theorem 6.1. □

Remark 6.4. Theorem 6.1 shows that there exists a uniform bound on the absolute error between the estimate of the input to the plant and the prescribed control input for each manipulated variable. This result establishes a sufficient condition for FDI: if the bound is breached, then an actuator fault must have taken place. The design allows for "small" faults, which are indistinguishable from the effect of the system uncertainty, to go undetected; however, such faults, since they essentially have the same effect as the system uncertainty, may be handled by the robustness of the control design.

We then consider a case where Assumption 6.1 is satisfied and derive time-varying bounds (in the discrete-time domain) on the outputs of the actuators for FDD. To this end, we first derive bounds on $F_{d,k}$. Define $\theta_{d,i,l}$ and $\theta_{d,i,u}$ in the same way as $\theta_{i,l}$ and $\theta_{i,u}$ were defined in Section 6.2.2, for $i = 1, \ldots, m$. It follows that

$$\int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,l}) dt \leq F_{d,i,k} \leq \int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,u}) dt \tag{6.12}$$

Let $f_{d,i,k,l} = \int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,l})dt$ and $f_{d,i,k,u} = \int_{t_k}^{t_{k+1}} f_{d,i}(x, \theta_{d,i,u})dt$ denote the lower and upper bounds on $F_{d,i,k}$, respectively. The FDD scheme using time-varying thresholds is formalized in Theorem 6.2 below.

Theorem 6.2. *Consider the system of Eq. (6.1), for which Assumptions 6.1 and 6.3 hold. Then, there exist $u_{i,k,l}$ and $u_{i,k,u}$ such that if $u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}]$, then $\tilde{u}_i(t_k) \neq 0$, and $u_i(t_k) + \tilde{u}_i(t_k) \in [u_{i,k,l}, u_{i,k,u}]$.*

Proof. It follows from Eq. (6.8) that

$$\begin{aligned} u_i(t_k) + \tilde{u}_i(t_k) &= [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k)] - \sum_{j=1}^{m}[G_{d,k}^{-1}]_{ij}F_{d,j,k} \\ &\geq [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k)] - \sum_{j=1}^{m}[G_{d,k}^{-1}]_{ij}F_{d,j,k,l} \end{aligned} \tag{6.13}$$

where $F_{d,j,k,l} = \begin{cases} f_{d,j,k,l}, & \text{if } [G_{d,k}^{-1}]_{ij} \leq 0 \\ f_{d,j,k,u}, & \text{if } [G_{d,k}^{-1}]_{ij} > 0 \end{cases}, j = 1, \ldots, m$. Let $F_{d,k,l} = [F_{d,1,k,l}, \ldots, F_{d,m,k,l}]^{\mathrm{T}}$. Then, we have that

$$u_i(t_k) + \tilde{u}_i(t_k) \geq [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k,l}] \tag{6.14}$$

Similarly, we have that

$$u_i(t_k) + \tilde{u}_i(t_k) \leq [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k,u}] \tag{6.15}$$

where $F_{d,k,u} = [F_{d,1,k,u}, \ldots, F_{d,m,k,u}]^{\mathrm{T}}$, with $F_{d,j,k,u} = \begin{cases} f_{d,j,k,u}, & \text{if } [G_{d,k}^{-1}]_{ij} \leq 0 \\ f_{d,j,k,l}, & \text{if } [G_{d,k}^{-1}]_{ij} > 0 \end{cases}, j = 1, \ldots, m$. Let $u_{i,k,l} = [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k,l}]$ and $u_{i,k,u} = [G_{d,k}^{-1}]_i[x_d(t_{k+1}) - x_d(t_k) - F_{d,k,u}]$. Thus, $u_{i,k,l} \leq u_i(t_k) + \tilde{u}_i(t_k) \leq u_{i,k,u}$, and $u_{i,k,l} \leq u_i(t_k) \leq u_{i,k,u}$ if $\tilde{u}_i(t_k) = 0$. Therefore, $u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}]$ implies that $\tilde{u}_i(t_k) \neq 0$. This concludes the proof of Theorem 6.2. □

Remark 6.5. In Theorem 6.2, the monotonic property of the right-hand side of the state equation with respect to the uncertain variables is utilized to generate time-varying bounds on the actual input to the plant. In the absence of faults, the actual input is equal to its prescribed value, which should reside within the set dictated by the estimated bounds on the actual input, for each manipulated variable. If the prescribed value breaches these bounds for some manipulated variable, the only way that it can happen is when the actual input is

no longer equal to the prescribed value, resulting in the detection and isolation of a fault. Note that while faults that do not lead to $u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}]$ cannot be detected, they may be handled through the robustness of the control design. Note also that beyond FDI, the fault diagnosis scheme provides an estimate of the output of the failed actuator.

The FDD procedure for the case where an actuator seizes at an arbitrary position is summarized as follows:

1. At time t_{k+1}, $k = 0, \ldots, \infty$, compute $u_{i,k,l}$ and $u_{i,k,u}$, $i = 1, \ldots, m$.

2. Let
$$r_{b,i,k} := \begin{cases} 1, & \text{if } u_i(t_k) \notin [u_{i,k,l}, u_{i,k,u}] \\ 0, & \text{otherwise} \end{cases} \tag{6.16}$$
where $r_{b,i,k}$ denotes a binary residual for u_i. If n_d non-zero residuals for u_i are monitored consecutively, where n_d is a design parameter for FDD, report a fault at time $t_d = t_{k+1}$ for the actuator that corresponds to u_i and choose $\bar{u}_{i,l} = \max \cup_{j\in\{k+1-n_d,\ldots,k\}} \{u_{i,j,l}\} \cup \{u_{i,\min}\}$ and $\bar{u}_{i,u} = \min \cup_{j\in\{k+1-n_d,\ldots,k\}} \{u_{i,j,u}\} \cup \{u_{i,\max}\}$ as the lower and upper bounds on the failed actuator position, respectively. Otherwise, repeat step 1.

6.3.2 Handling State Estimation Errors for Fault Diagnosis

In many practical situations, it is not economical to measure all the system states, or in some situations, only part of the system states are inherently measurable, which necessitates output feedback control by using state estimators. In this section, we generalize the fault diagnosis scheme of Section 6.3.1 to handle state estimation errors, with the focus on the problem of FDD (and not the state estimator design). To this end, we assume the existence of a state estimator (observer or predictor) which can provide the state estimate, denoted by $\hat{x}(t)$ at time t, that is accurate enough (at least for some time even after an actuator fault takes place) to perform fault diagnosis (see Remark 6.6 for examples of such observers). This is formalized in Assumption 6.4 below [27].

Assumption 6.4. For the system of Eq. (6.1), there exists a state estimator such that given positive real numbers e and $\tilde{u}_b$, there exists $t_e > 0$ such that if $\|\tilde{u}(t)\| \leq \tilde{u}_b$, then $\|x(t) - \hat{x}(t)\| \leq e$ for all $t \in [t_e, \infty)$. Furthermore, there exists $T_d > 0$ such that if $\|\tilde{u}(t)\| > \tilde{u}_b$ for some $t_f > t_e$, then $\|x(t) - \hat{x}(t)\| \leq e$ for all $t \in [t_e, t_f + T_d]$.

The key idea of the FDD design for the case with state estimation errors is to use the state estimate and the bounds on uncertainty and the estimation errors to determine the bounds on $u(t_k) + \tilde{u}(t_k)$ as in Section 6.3.1, which is formalized in Theorem 6.3 below. To this end, let $\hat{F}_{d,k} = \int_{t_k}^{t_{k+1}} f_d(\hat{x}, \theta(t))dt$, $\hat{G}_{d,k} = \int_{t_k}^{t_{k+1}} G_d(\hat{x})dt$, $\hat{F}_{d,i,k}$ denote the ith element of $\hat{F}_{d,k}$, and $\hat{G}_{d,i,k}$ denote the ith row of $\hat{G}_{d,k}$. The lower and upper bounds on $\hat{F}_{d,i,k}$, denoted by $\hat{f}_{d,i,k,l}$ and $\hat{f}_{d,i,k,u}$, can be computed in the same way as $f_{d,i,k,l}$ and $f_{d,i,k,u}$ in Section 6.3.1 by using $\hat{x}$ instead of x.

Theorem 6.3. *Consider the system of Eq. (6.1) subject to state estimation errors, for which Assumptions 6.1 and 6.4 hold. Assume that $m \leq n$ and $\hat{G}_{d,k}$ is invertible for $k = 0, \ldots, \infty$. Then, for $[t_k, t_{k+1}] \subseteq [t_e, t_f + T_d]$, there exist $\gamma = [\gamma_1, \ldots, \gamma_m]^{\mathrm{T}} > 0$, $\hat{u}_{i,k,l}(\gamma)$, and $\hat{u}_{i,k,u}(\gamma)$ such that if $u_i(t_k) \notin [\hat{u}_{i,k,l}(\gamma), \hat{u}_{i,k,u}(\gamma)]$, then $\tilde{u}_i(t_k) \neq 0$, and $u_i(t_k) + \tilde{u}_i(t_k) \in [\hat{u}_{i,k,l}(\gamma), \hat{u}_{i,k,u}(\gamma)]$.*

Proof. It follows from Eq. (6.7) that $F_{d,i,k} = x_{d,i}(t_{k+1}) - x_{d,i}(t_k) - G_{d,i,k}[u(t_k) + \tilde{u}(t_k)]$. Similarly, define $\tilde{F}_{d,i,k} = \hat{x}_{d,i}(t_{k+1}) - \hat{x}_{d,i}(t_k) - \hat{G}_{d,i,k}[u(t_k) + \tilde{u}(t_k)]$, where $\hat{x}_{d,i}$ denotes the estimate of $x_{d,i}$. Since $\|x(t) - \hat{x}(t)\| \leq e$ for all $t \in [t_k, t_{k+1}]$ under Assumption 6.4 and $G(x)$ is locally Lipschitz, there exists $L_{g,i} > 0$ such that $\|\hat{G}_{d,i,k}^{\mathrm{T}} - G_{d,i,k}^{\mathrm{T}}\| \leq L_{g,i}\Delta e$. It follows that

$$\begin{aligned} |\tilde{F}_{d,i,k} - F_{d,i,k}| &\leq |\hat{x}_{d,i}(t_{k+1}) - x_{d,i}(t_{k+1})| + |\hat{x}_{d,i}(t_k) - x_{d,i}(t_k)| \\ &\quad + \left|(\hat{G}_{d,i,k} - G_{d,i,k})[u(t_k) + \tilde{u}(t_k)]\right| \\ &\leq 2e + L_{g,i}u_b\Delta e \end{aligned} \tag{6.17}$$

The above equation leads to

$$F_{d,i,k} - (2 + L_{g,i}u_b\Delta)e \leq \tilde{F}_{d,i,k} \leq F_{d,i,k} + (2 + L_{g,i}u_b\Delta)e \tag{6.18}$$

Since $f_d(x, \theta)$ is locally Lipschitz in x, there exists $L_{f,i} > 0$ such that $|F_{d,i,k} - \hat{F}_{d,i,k}| \leq L_{f,i}\Delta e$, which leads to

$$\hat{F}_{d,i,k} - L_{f,i}\Delta e \leq F_{d,i,k} \leq \hat{F}_{d,i,k} + L_{f,i}\Delta e \tag{6.19}$$

Note that $\hat{f}_{d,i,k,l} \leq \hat{F}_{d,i,k} \leq \hat{f}_{d,i,k,u}$. Then, Eqs. (6.18) and (6.19) yield

$$\hat{f}_{d,i,k,l} - \gamma_i \leq \tilde{F}_{d,i,k} \leq \hat{f}_{d,i,k,u} + \gamma_i \tag{6.20}$$

where $\gamma_i = (2 + L_{f,i}\Delta + L_{g,i}u_b\Delta)e$. Since $\hat{G}_{d,k}$ is invertible, we have $u_i(t_k) + \tilde{u}_i(t_k) = [\hat{G}_{d,k}^{-1}]_i[\hat{x}_d(t_{k+1}) - \hat{x}_d(t_k) - \tilde{F}_{d,k}]$, where $[\hat{G}_{d,k}^{-1}]_i$ denotes the ith row of $\hat{G}_{d,k}^{-1}$, $\hat{x}_d = [\hat{x}_{d,1}, \ldots, \hat{x}_{d,m}]^{\mathrm{T}}$, and $\tilde{F}_{d,k} = [\tilde{F}_{d,1,k}, \ldots, \tilde{F}_{d,m,k}]^{\mathrm{T}}$. Now, with the bounds on $\tilde{F}_{d,i,k}$ computed, the rest of the proof proceeds along the same lines as the proof of Theorem 6.2. This concludes the proof of Theorem 6.3. □

Remark 6.6. In the context of output feedback control, the fault diagnosis scheme of Theorem 6.3 requires that the structure of the system allow the design of a state estimator that can provide an accurate enough state estimate. Examples of such estimators include a high-gain state observer (see, e.g., [27]) and a reduced-order nonlinear observer developed in [82].

6.4 Robust Safe-Parking for Fault-Tolerant Control

In this section, we consider the problem of fault-handling for the case where an actuator seizes at an arbitrary position (and does not revert to the pre-designed fail-safe position). The key idea of the proposed approach is to design safe-park point candidates off-line for a series of the output values of the potential failed actuator, and upon FDD, choose a safe-park point on-line such that the system can be stabilized at the chosen safe-park point by the robust control law, which can handle the error between the actual value of the failed actuator position and its design counterpart.

Specifically, we design safe-park point candidates for M actuator positions of u_i denoted by $\bar{u}_{s,i,j} \in [u_{i,\min}, u_{i,\max}], j = 1, \ldots, M$. When designing the control law and characterizing the stability region of a safe-park point candidate, a design uncertain variable of magnitude δ_s (over and above the uncertain variables in the system description) is used to account for the error between the actual value of the failed actuator position, denoted by $\bar{u}_{i,f}$, and the one used to design the safe-park point candidate ($\bar{u}_{s,i,j}$). Let u_{nom} and $u_{s,i,j}$ denote the control laws to stabilize the system at the nominal equilibrium point x_{nom} and a safe-park point $x_{s,i,j}$, respectively, yielding Ω_{nom} and $\Omega_{s,i,j}$ as their stability regions. The schematic in Fig. 6.1 shows the integrated fault diagnosis and safe-parking framework, which is formalized in Theorem 6.4 below (the proof of this theorem follows a similar line of argument as in [74] and is omitted).

Theorem 6.4. *Consider the system of Eq. (6.1) under a control law $RC(x)$ satisfying Assumption 6.2. Let t_f be the time when a fault takes place, t_d the time when it is detected and diagnosed, and t_r the time when it is repaired. If $x(0) \in \Omega_{nom}$, $[\bar{u}_{i,l}, \bar{u}_{i,u}] \subseteq [\bar{u}_{s,i,j} - \delta_s, \bar{u}_{s,i,j} + \delta_s]$, $x(t_d) \in \Omega_{s,i,j}$, and $B_{d,s,i,j} \subseteq \Omega_{nom}$, where $B_{d,s,i,j}$ is a closed ball of radius d around $x_{s,i,j}$, then the switching rule*

$$u(t) = \begin{cases} u_{nom}(t), & 0 \leq t < t_d \\ u_{s,i,j}(t), & t_d \leq t < t_s \\ u_{nom}(t), & t_s \leq t \end{cases} \tag{6.21}$$

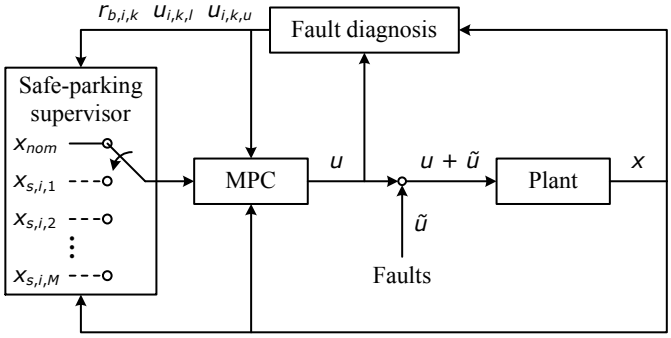

Figure 6.1: Schematic of the integrated fault diagnosis and safe-parking framework.

where $t_s \geq t_r$ is such that $x(t_s) \in \Omega_{nom}$, guarantees that $x(t) \in \Omega_{nom}\ \forall\ t \in [0, t_f] \cup [t_s, \infty)$ and there exists a positive real number T_f such that $\|x(t)\| \leq d$ for all $t \geq T_f$.

Remark 6.7. Upon the confirmation of a fault, the safe-parking mechanism described by Theorem 6.4 is activated to shift the control objective from operating the system at the nominal equilibrium point to maintaining it at a suboptimal but admissible operating point. Note that a safe-park point is chosen from the candidates generated for the design value of the failed actuator position $\bar{u}_{s,i,j}$ such that the range $[\bar{u}_{s,i,j} - \delta_s, \bar{u}_{s,i,j} + \delta_s]$ designed off-line contains the range $[\bar{u}_{i,l}, \bar{u}_{i,u}]$ identified on-line for the failed actuator position, as illustrated in Fig. 6.2. Since $[\bar{u}_{i,l}, \bar{u}_{i,u}]$ contains the actual value of the failed actuator position $\bar{u}_{i,f}$, it is guaranteed that such a safe-park point candidate is a feasible equilibrium point subject to the fault. Note also that an arbitrarily chosen safe-park point candidate is not guaranteed to be a feasible equilibrium point in the presence of the fault. Therefore, the fault information provided by the fault diagnosis design is essential in choosing a safe-park point.

Remark 6.8. The remaining conditions dictating the choice of a safe-park point follow from the safe-parking framework designed for a fail-safe position in [74]. In particular, to make sure that the system can be driven to the temporary operating point, it requires that the system state should reside within the stability region of the safe-park point at the time of fault confirmation. Note that t_s denotes a time when the system state is within the stability region of the nominal equilibrium point after the fault is repaired. If it is already within the stability region of the nominal equilibrium point at the time of fault repair, then $t_s = t_r$. Otherwise, the control action is implemented to drive the system state to the safe-park point until it reaches the stability region of the nominal equilibrium point. Note in general that the possibility of finding safe-park points and resuming normal operation can be enhanced by the use of control designs (or Lyapunov functions) that yield as large a stability region for the nominal (and safe-parking) operation as possible. The size of the

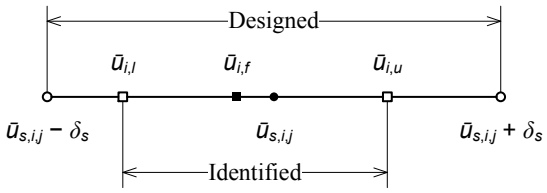

Figure 6.2: Schematic illustrating the choice of a safe-park point. The range $[\bar{u}_{s,i,j} - \delta_s, \bar{u}_{s,i,j} + \delta_s]$ is designed off-line for the actuator position $\bar{u}_{s,i,j}$ with the robustness margin δ_s. The range $[\bar{u}_{i,l}, \bar{u}_{i,u}]$ is identified on-line, which contains the actual value of the failed actuator position $\bar{u}_{i,f}$.

stability region remains case-specific; however, the ability to explicitly characterize the stability region (provided by the control design used in this chapter) is useful in ascertaining the ability of the controller to best utilize the available control effort and design the safe-parking framework.

Remark 6.9. It should be noted that the safe-parking mechanism of Theorem 6.4 can be extended to handle the case with limited availability of measurements by following the same idea in [75]. Due to the lack of full state measurements, a safe-park point should be chosen based on the state estimate. It is shown in [75] that once the state estimation error falls below a certain value, the presence of the system state within an appropriate subset of the stability region obtained under state feedback control guarantees that it is within the stability region for the case with limited measurements. Therefore, the key consideration in the implementation of the safe-parking framework is to make the choice of a safe-park point only after the state estimation error becomes sufficiently small.

6.5 Simulation Example

In this section, we illustrate the proposed fault diagnosis techniques and the generalized safe-parking framework via a CSTR example, as shown in Fig. 6.3, where three parallel irreversible elementary exothermic reactions of the form $A \xrightarrow{k_1} B$, $A \xrightarrow{k_2} U$, and $A \xrightarrow{k_3} R$ take place, with A being the reactant species, B the desired product, and U and R the undesired byproducts. The feed to the reactor consists of reactant A at a flow rate F, concentration C_{A0}, and temperature T_0. Under standard assumptions, the mathematical model of the process can be derived from material and energy balances, which takes the following

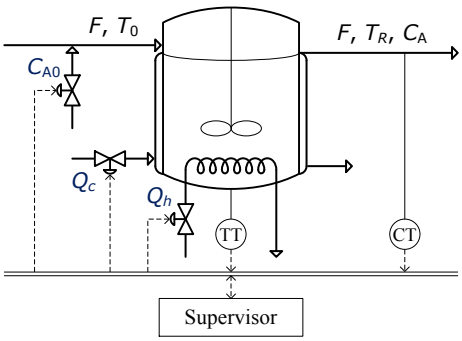

Figure 6.3: Schematic of the chemical reactor example of Section 6.5.

form:

$$\begin{aligned}\dot{C}_{\mathrm{A}} &= \frac{F}{V}(C_{\mathrm{A0}} - C_{\mathrm{A}}) - \sum_{i=1}^{3} R_i(C_{\mathrm{A}}, T_R) \\ \dot{T}_R &= \frac{F}{V}(T_0 - T_R) + \sum_{i=1}^{3} \frac{(-\Delta H_i)}{\rho c_p} R_i(C_{\mathrm{A}}, T_R) + \frac{Q}{\rho c_p V}\end{aligned} \tag{6.22}$$

where $R_i(C_{\mathrm{A}}, T_R) = k_{i0} e^{-E_i/RT_R} C_{\mathrm{A}}$ for $i = 1, 2, 3$, C_{A} is the concentration of species A in the reactor, T_R is the temperature of the reactor, Q is the rate of heat input to the reactor, V is the volume of the reactor, k_{i0}, E_i, and ΔH_i are the pre-exponential constant, the activation energy, and the enthalpy of reaction i, respectively, and c_p and ρ are the heat capacity and density of the reacting mixture, respectively. The process parameters can be found in Table 6.1.

Under fault-free conditions, the control objective is to stabilize the reactor at the unstable equilibrium point $(C_{\mathrm{A}}, T_R) = (3.50\,\mathrm{kmol/m^3}, 405.0\,\mathrm{K})$, denoted by N in Fig. 6.4, by manipulating C_{A0} and Q, where $0 \leq C_{\mathrm{A0}} \leq 6\,\mathrm{kmol/m^3}$ and $-8\times10^5\,\mathrm{kJ/hr} \leq Q \leq 8\times10^5\,\mathrm{kJ/hr}$. The manipulated variable $Q = Q_c + Q_h$, where Q_c and Q_h denote cooling and heating, respectively, with $-8 \times 10^5\,\mathrm{kJ/hr} \leq Q_c \leq 0$ and $0 \leq Q_h \leq 8 \times 10^5\,\mathrm{kJ/hr}$. The nominal steady-state values of the manipulated variables are $C_{\mathrm{A0}} = 4.25\,\mathrm{kmol/m^3}$ and $Q = -6.55 \times 10^4\,\mathrm{kJ/hr}$. The simulations are conducted under a 0.5% error in the pre-exponential constant (k_{10}) for the main reaction and sinusoidal disturbances in the feed temperature (T_0) with an amplitude of 3 K and a period of 0.2 hr. The bounds on the errors in k_{10} and T_0 used in the monitoring and control design are $\pm1.5\%$ and ±5 K, respectively. The concentration and temperature measurements are assumed to have a truncated gaussian noise with a standard deviation of $0.01\,\mathrm{kmol/m^3}$ and 0.1 K for the parent normal distribution, respectively. The lower and upper truncation points are -0.02 and $0.02\,\mathrm{koml/m^3}$ for the concentration, and -0.2 and 0.2 K for the temperature, respectively.

Table 6.1: Process parameters for the chemical reactor example of Section 6.5.

Parameter	Value	Unit
F	4.998	m^3/hr
T_0	300.0	K
V	1.0	m^3
R	8.314	kJ/kmol·K
k_{10}	3.0×10^6	hr^{-1}
k_{20}	3.0×10^5	hr^{-1}
k_{30}	3.0×10^5	hr^{-1}
E_1	5.00×10^4	kJ/kmol
E_2	7.53×10^4	kJ/kmol
E_3	7.53×10^4	kJ/kmol
ΔH_1	-5.0×10^4	kJ/kmol
ΔH_2	-5.2×10^4	kJ/kmol
ΔH_3	-5.4×10^4	kJ/kmol
c_p	0.231	kJ/kg·K
ρ	1000.0	kg/m^3

The measurements are filtered before performing fault diagnosis and control calculations as $x_f(t_{k+1}) = 0.25x_f(t_k) + 0.75x_m(t_{k+1})$, where x_f and x_m denote the filtered state and noisy measurement, respectively.

To demonstrate the efficacy of the integrated fault diagnosis and safe-parking framework, we consider a failure in the actuator used to control Q_c. The safe-park point candidates are shown in Table 6.2 for 6 actuator positions of Q_c with a robustness margin $\delta_s = 1.25 \times 10^4$ kJ/hr. In the control law of Eq. (6.4), an execution time $\Delta = 0.025$ hr $= 1.5$ min and a prediction horizon of 2Δ are used, with $Q_w = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 10 \end{smallmatrix}\right]$ and $R_w = \left[\begin{smallmatrix} 10^5 & 0 \\ 0 & 10^{-6} \end{smallmatrix}\right]$. The Lyapunov function used to characterize the stability region and to prescribe the control input for the nominal equilibrium point is chosen as $V(x) = x^T P x$, where $P = \left[\begin{smallmatrix} 7.72\times10^{-1} & 0 \\ 0 & 4\times10^{-4} \end{smallmatrix}\right]$, and those for the safe-park point candidates can be found in Table 6.2. It is assumed that there are 20 samplings during one execution period (i.e., the sampling time is 4.5 sec). The trapezoidal rule is used to compute the integrals for the estimation of the bounds on the actual input to the plant. To account for measurement noise, the lower and upper bounds on the estimates of C_{A0} and Q implemented to the plant under state feedback control are relaxed by a magnitude of 0.32 $kmol/m^3$ and 1848 kJ/hr (inferred from process data under healthy conditions), respectively.

We first consider a case where full state measurements are available and the process starts from an initial condition at $O_1(2.50\ kmol/m^3, 405.0\ K)$. The actuator fails at time

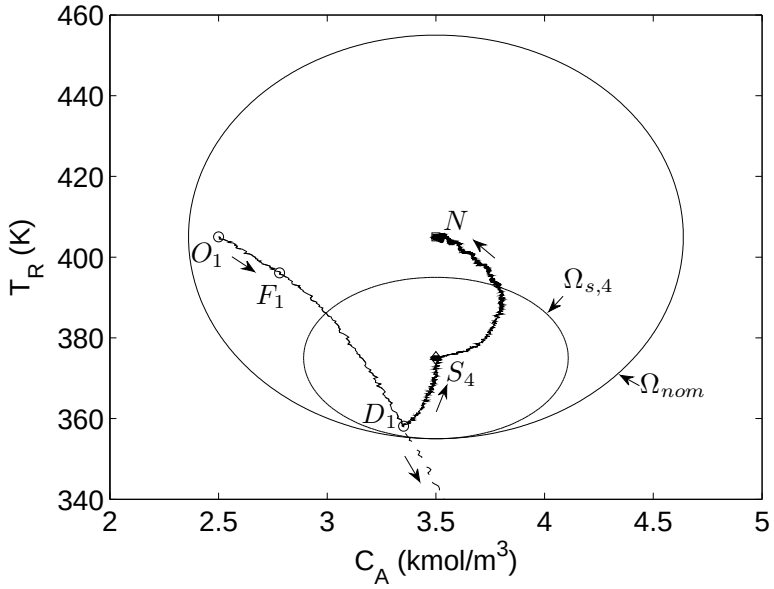

Figure 6.4: Closed-loop state trajectories for the chemical reactor example where the process starts from O_1 and the cooling valve fails at F_1. The solid line shows the case where the fault is confirmed at D_1, the process is stabilized at the safe-park point S_4, and nominal operation is resumed upon fault repair. The dashed line shows process instability when no fault-handling mechanism is implemented. The arrows show the directions of the trajectories.

$t_f = 0.05$ hr, with the process state at $F_1(2.78\ \text{kmol/m}^3, 396.1\ \text{K})$. The output value of the failed actuator is $\bar{u}_f = -4.19 \times 10^4$ kJ/hr (the same as it was at time t_f^-) during fault repair. The FDD scheme can be explained by Fig. 6.5, where the prescribed inputs are marked by crosses, the actual inputs marked by circles, and the estimated bounds on the actual inputs marked by error bars. Note that a fault is declared when the prescribed value breaches the bounds identified from state measurements. It can be seen that the fault in Q_c is first declared at 0.1 hr (i.e., there is a two-step time delay). Upon the first alarm, the actuator for Q_h is disabled (i.e., the prescribed value of Q_h is 0) to allow FDD for Q_c until the fault is confirmed to be true or false (this step is necessitated by the fact that the FDD scheme cannot differentiate between faults in Q_c and Q_h since they affect the system in an identical fashion). The fault is confirmed at time $t_d = 0.175$ hr after 4 consecutive alarms (i.e., $n_d = 4$), with the process state at $D_1(3.35\ \text{kmol/m}^3, 358.1\ \text{K})$. The binary residuals for the manipulated variables C_{A0} and Q are shown in Figs. 6.6(a) and 6.6(b), respectively, while the residuals of the manipulated variables obtained by using the nominal process model are shown in Figs. 6.6(c) and 6.6(d), where the thresholds (see the dashed lines) are 0.5 kmol/m^3 and 1.5×10^4 kJ/hr, respectively. It can be seen that similar results are obtained by the FDI designs using constant and time-varying thresholds, with no false

Table 6.2: Safe-park point candidates, steady-state values of the manipulated variables, and Lyapunov functions for the chemical reactor example of Section 6.5 ($\alpha = 1.25$).

Safe-park point candidates	Q_c (10^4 kJ/hr)	C_A (kmol/m^3)	T_R (K)	C_{A0} (kmol/m^3)	Q (10^4 kJ/hr)	P $V(x) = x^T P x$
S_1	$-6.55 \pm \alpha$	3.50	380	3.78	2.21	$\begin{bmatrix} 2.7 & 0 \\ 0 & 2.5\times10^{-3} \end{bmatrix}$
S_2	$-5.73 \pm \alpha$	3.85	375	4.10	2.40	$\begin{bmatrix} 2.7 & 0 \\ 0 & 2.5\times10^{-3} \end{bmatrix}$
S_3	$-4.91 \pm \alpha$	3.50	380	3.78	2.21	$\begin{bmatrix} 2.7 & 0 \\ 0 & 3.5\times10^{-3} \end{bmatrix}$
S_4	$-4.10 \pm \alpha$	3.50	375	3.73	2.97	$\begin{bmatrix} 2.7 & 0 \\ 0 & 2.5\times10^{-3} \end{bmatrix}$
S_5	$-3.28 \pm \alpha$	3.50	375	3.73	2.97	$\begin{bmatrix} 2.7 & 0 \\ 0 & 3.5\times10^{-3} \end{bmatrix}$
S_6	$-2.46 \pm \alpha$	3.85	375	4.10	2.40	$\begin{bmatrix} 5.0 & 0 \\ 0 & 7.0\times10^{-3} \end{bmatrix}$

alarms generated.

Beyond FDI, the fault diagnosis scheme also identifies the lower and upper bounds on the actual value of the failed actuator position, which are -5.00×10^4 kJ/hr and -3.81×10^4 kJ/hr, respectively. This information is then used to choose a safe-park point. By referring to Table 6.2, it is found that the safe-park point candidate S_4(3.50 kmol/m^3, 375 K) is designed for the case where the cooling valve seizes at some value in $[-5.35 \times 10^4$ kJ/hr, -2.85×10^4 kJ/hr$]$, which contains $[-5.00 \times 10^4$ kJ/hr, -3.81×10^4 kJ/hr$]$. Note that the process state at time t_d is also within the stability region of S_4, denoted by $\Omega_{s,4}$. Therefore, S_4 is chosen as a safe-park point. As shown by the solid line in Fig. 6.4, if the safe-parking strategy is implemented, the process is first stabilized at S_4, and nominal operation is resumed upon fault repair. The absence of an appropriately designed fault-handling framework, however, results in process instability, as shown by the dashed line in Fig. 6.4. The corresponding state and input profiles are shown in Fig. 6.7.

We then consider a case where concentration measurements are only available every 10Δ. For this case, we study the problem of estimating the output of the failed actuator and using its estimate to implement the safe-parking operation, with the focus on the diagnosis of the fault magnitude for a fault in Q. The concentration between consecutive measurements is predicted by using the nominal process model and temperature measurements as follows:

$$\begin{aligned} \dot{\hat{C}}_A &= \frac{F}{V}(C_{A0} - \hat{C}_A) - \sum_{i=1}^{3} R_i(\hat{C}_A, T_R) \\ \hat{C}_A(10k\Delta) &= C_A \end{aligned} \tag{6.23}$$

where $\hat{C}_A$ denotes the estimate of the concentration, which is set to its true value each time an asynchronous measurement is available. In the fault diagnosis design, $\gamma = [0.04, 0.2]^T$

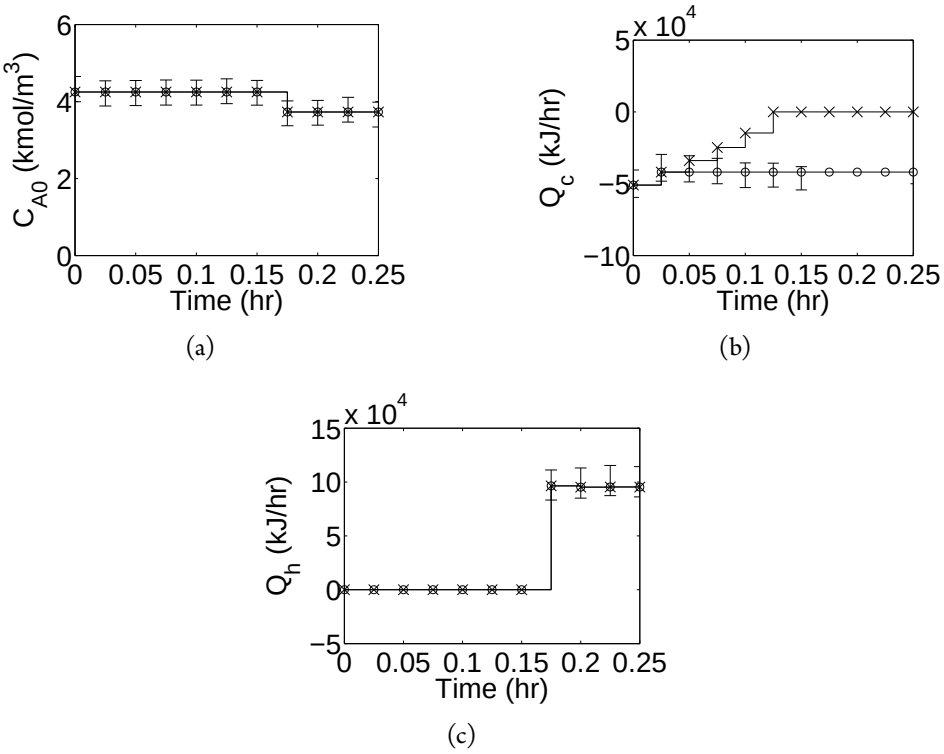

Figure 6.5: Illustration of the FDD scheme of Theorem 6.2 for the chemical reactor example. The cooling valve fails at time 0.05 hr. The fault is first detected and isolated at 0.1 hr and confirmed at 0.175 hr after 4 consecutive alarms. Crosses denote the prescribed inputs, circles denote the implemented inputs, and error bars denote the estimated bounds on the actual inputs for (a) C_{A0}, (b) Q_c, and (c) Q_h.

is used to relax the bounds on the estimate of the actual input to the plant. As shown in Fig. 6.8, the process starts from $O_2(4.25\ \text{kmol/m}^3, 390\ \text{K})$. The fault in Q_c takes place at time $t_f = 0.05$ hr, with the actuator frozen at -2.59×10^4 kJ/hr and the process state at $F_2(4.14\ \text{kmol/m}^3, 389.1\ \text{K})$. The fault is first detected and isolated at time 0.125 hr and confirmed after 4 consecutive alarms at time $t_d = 0.2$ hr, as shown in Fig. 6.9, with the process state at $D_2(4.01\ \text{kmol/m}^3, 369.4\ \text{K})$. It can be seen from Fig. 6.9 that the estimate of the failed actuator output is $[-3.60 \times 10^4, -2.17 \times 10^4]$, which is a subset of $[-3.71 \times 10^4, -1.21 \times 10^4]$ designed for $S_6(3.85\ \text{kmol/m}^3, 375\ \text{K})$ in Table 6.2. Because D_2 also resides within the stability region of S_6, denoted by $\Omega_{s,6}$, S_6 is chosen as a safe-park point. As shown in Fig. 6.8, the process operates at S_6 during fault repair until nominal operation is resumed at $t_r = 1.5$ hr. The corresponding state and input profiles are depicted in Fig. 6.10.

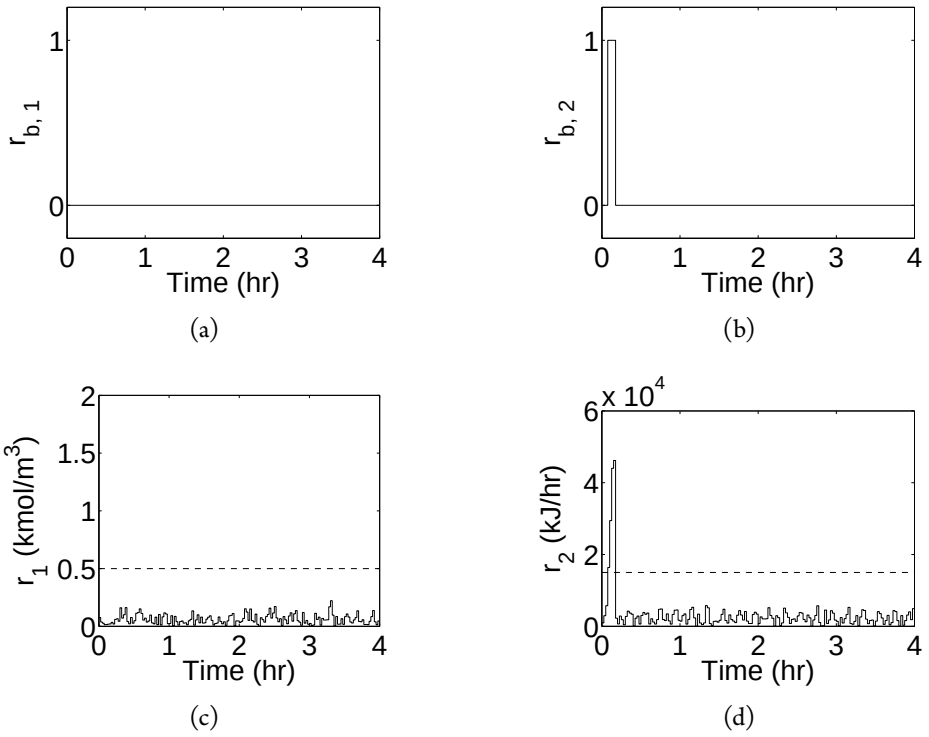

Figure 6.6: (a, b) Binary residuals defined by Eq. (6.16) and (c, d) residuals defined by Eq. (6.9) for manipulated variables C_{A0} and Q, respectively, in the chemical reactor example.

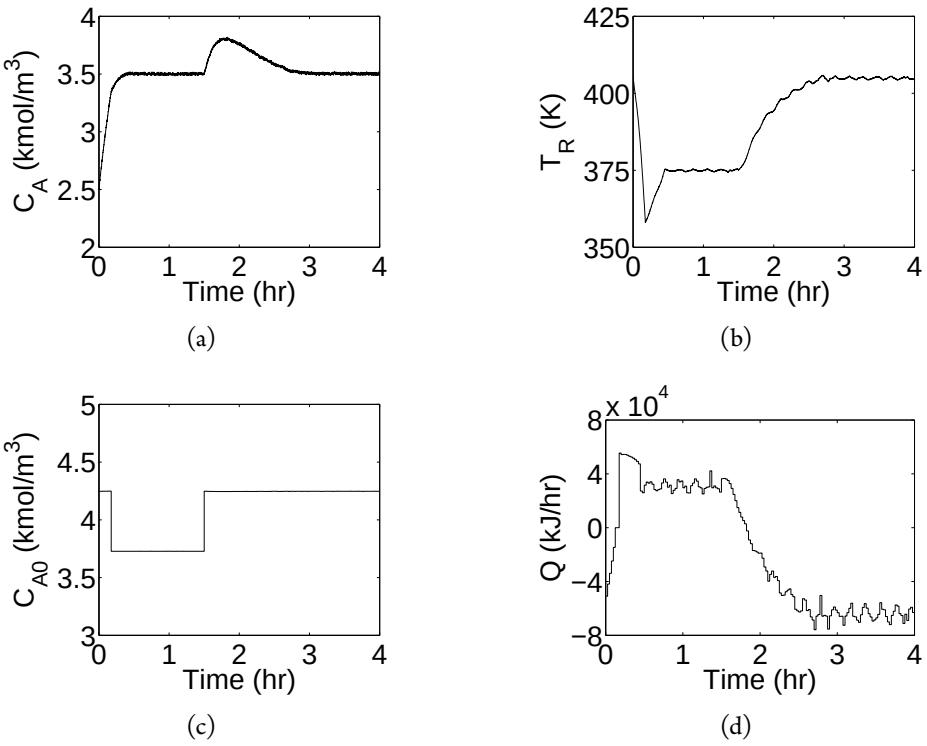

Figure 6.7: (a, b) Closed-loop state and (c, d) input profiles for the chemical reactor example. The safe-parking operation starts from 0.175 hr, and nominal operation is resumed at 1.5 hr.

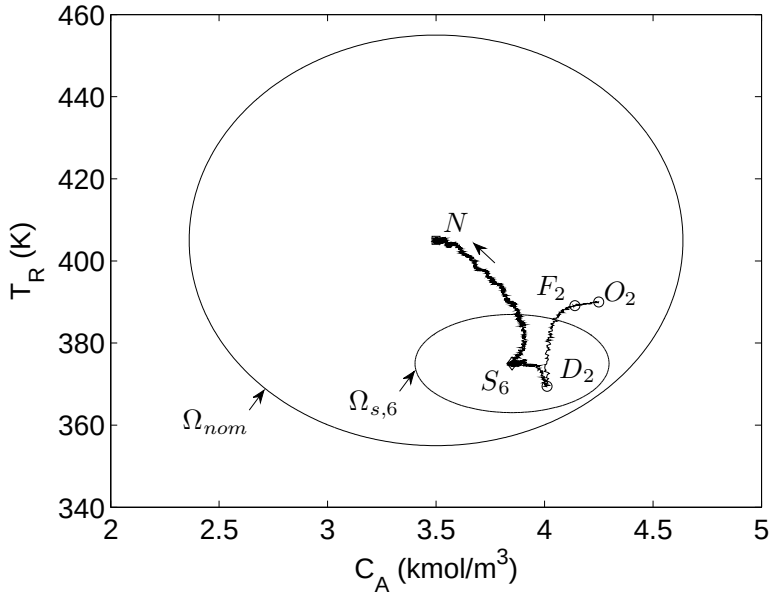

Figure 6.8: Closed-loop state trajectory for the chemical reactor example with asynchronous concentration measurements where the process starts from O_2 and the cooling valve fails at F_2. The fault is confirmed at D_2, the process is stabilized at the safe-park point S_6, and nominal operation is resumed upon fault repair. The arrow shows the direction of the trajectory.

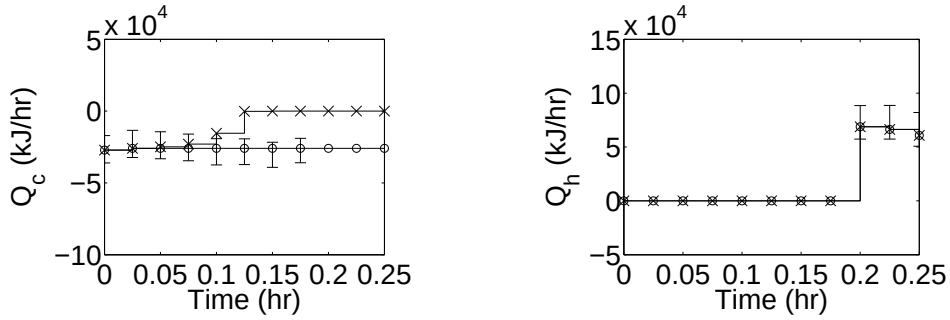

Figure 6.9: Illustration of the FDD scheme of Theorem 6.3 for the chemical reactor example with asynchronous concentration measurements. The cooling valve fails at time 0.05 hr. The fault is first detected and isolated at 0.125 hr and confirmed at 0.2 hr after 4 consecutive alarms. Crosses denote the prescribed inputs, circles denote the implemented inputs, and error bars denote the estimated bounds on the actual inputs for (a) Q_c and (b) Q_h.

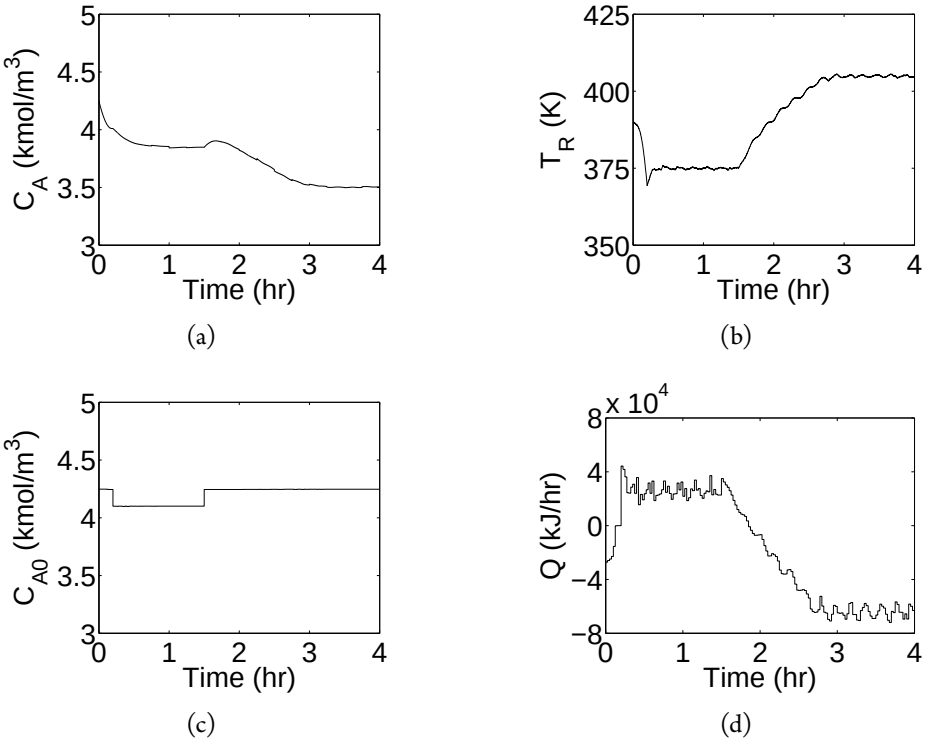

Figure 6.10: (a, b) Closed-loop state and (c, d) input profiles for the chemical reactor example with asynchronous concentration measurements. The safe-parking operation starts from 0.2 hr, and nominal operation is resumed at 1.5 hr.

6.6 Conclusions

This chapter considered the problem of designing an integrated fault diagnosis and safe-parking framework to deal with actuator faults in nonlinear process systems. To this end, a model-based fault diagnosis design was first proposed, which can not only identify the failed actuator, but also estimate the fault magnitude. The fault information is obtained by estimating the outputs of the actuators and comparing them with the corresponding prescribed control inputs. This methodology was first developed under state feedback control and then generalized to deal with state estimation errors. In the safe-parking design, possible safe-park points are generated for a series of design values of the failed actuator position. After a fault is diagnosed, the estimate of the failed actuator position is used to choose a safe-park point. The discrepancy between the actual value of the failed actuator position and the corresponding design value is handled through the robustness of the control design. The efficacy of the integrated fault diagnosis and safe-parking framework was demonstrated through a chemical reactor example.

Chapter 7

Conclusions and Future Work

This chapter summarizes the main contributions of this thesis and suggests research opportunities for future work.

7.1 Conclusions

This thesis considered the problem of fault-diagnosis and FTC of chemical process systems with nonlinear dynamics. In Chapter 2, an active fault isolation method was proposed for nonlinear process systems subject to uncertainty. The key idea of the proposed method is to exploit the nonlinear way that faults affect the process evolution through supervisory control. To this end, a dedicated fault isolation residual and its time-varying threshold were generated for each fault by treating other faults as disturbances. A fault is isolated when the corresponding residual breaches its threshold. These residuals, however, may not be sensitive to faults under nominal operation. To make these residuals sensitive to faults, a switching rule was designed to drive the process states, upon detection of a fault using any fault detection methods, to move towards an operating point that, for any given fault, results in the reduction of the effect of other faults on the evolution of the same process state. This idea was then generalized to sequentially operate the process at multiple operating points that facilitate isolation of different faults. The effectiveness of the proposed method was illustrated using a chemical reactor example and demonstrated through application to a solution copolymerization of MMA and VAc.

In addition to actuator FDI, a sensor fault isolation and fault-tolerant control design was proposed for nonlinear systems subject to input constraints in Chapter 3. The key idea

of the proposed method is to exploit model-based sensor redundancy through state observer design. To this end, a high-gain observer was first presented and the stability property of the closed-loop system was rigorously established. By exploiting the enhanced applicability of the observer design, a fault isolation scheme was then proposed, which consists of a bank of observers, with each driven by a subset of the measured outputs. The residuals were defined as the discrepancies between the state estimates and their expected trajectories. A fault is isolated when all the residuals breach their thresholds except for the one that is generated without using measurements from the faulty sensor. After the fault is isolated, the state estimate generated using measurements from the healthy sensors is used in closed-loop to continue nominal operation. The implementation of the fault isolation and handling framework subject to uncertainty and measurement noise was illustrated using a chemical reactor example.

In Chapter 4, the problem of handling actuator faults was addressed for switched nonlinear process systems that transit between multiple modes subject to input constraints. The faults considered preclude the possibility of operation at the nominal equilibrium point in the active mode. Two cases were considered according to whether or not the switching schedule can be altered during the production process. For the case where the switching schedule is fixed, a safe-parking scheme was designed, which accounts for the switched nature, to operate the process at successive safe-park points as it transits to successive modes, which allow resumption of nominal operation after the fault is repaired. For the case where the switching schedule is adjustable, a safe-switching scheme was designed, which exploits the switched nature, to switch the process to a mode (if exists and available) where nominal operation can be preserved (through control structure reconfiguration when necessary) to continue nominal operation. The key ideas of the proposed framework were illustrated via a switched chemical reactor example, and the robustness with respect to uncertainty and measurement noise was demonstrated on an MMA polymerization process.

In Chapter 5, the safe-parking techniques developed for an isolated unit were generalized to account for the network structure of a chemical plant where multiple units are interconnected through an intricate network, with FDI and safe-parking techniques integrated in a unified framework. To this end, a robust FDI design was first presented, where relations between the prescribed inputs and state measurements in the absence of faults were constructed with the consideration of uncertainty. A fault is detected and isolated when the corresponding relation is violated. An algorithm was then developed to determine the units that need to be safe-parked during the fault repair period and generate possible safe-park points for the affected units. The implementation of the safe-parking techniques is

triggered by the isolation of a fault, which can localize the effect of the fault in a subsystem of the networked plant. The efficacy of the integrated FDI and safe-parking framework was demonstrated on a chemical process example comprising three reactors and a separator.

Finally, the assumption of the *a priori* knowledge about the position of the failed actuator was relaxed to consider the case where a failed actuator is frozen at an arbitrary position in Chapter 6. This problem was studied by integrating fault diagnosis and safe-parking techniques. To this end, a model-based fault diagnosis design was proposed, which can not only identify the failed actuator, but also estimate the fault magnitude. The fault information is obtained by estimating the outputs of the actuators and comparing them with the corresponding prescribed control inputs. This methodology was first developed under state feedback control and then generalized to deal with state estimation errors. In the safe-parking design, possible safe-park points were generated for a series of design values of the failed actuator position. After a fault is diagnosed, the estimate of the failed actuator position is used to choose a safe-park point. The discrepancy between the actual value of the failed actuator position and the corresponding design value is handled through the robustness of the control design. The efficacy of the integrated fault diagnosis and safe-parking framework was demonstrated through a chemical reactor example.

7.2 Future Work

The results of this thesis suggest the following topics for future work:

1. Fault diagnosis of nonlinear process systems subject to actuator and sensor faults.
2. Generalized sampled-data output feedback control using high-gain observers.
3. Application of the safe-parking approach to a medium scale nonlinear process example under output feedback control.

First, we consider the problem of fault diagnosis for nonlinear process systems subject to both actuator and sensor faults. In most existing results on model-based fault diagnosis (see also Chapters 2 and 3), the problem is studied for actuator and sensor faults separately. The implementation of these separately designed methods will likely result in the declaration of a fault in both actuator and sensor fault diagnosis systems. While engineering knowledge and experience could be used to find out the location of the failed equipment,

actuator and sensor faults should be simultaneously accounted for to automate the decision process. To address a commonly encountered faulty scenario, a maximum of two (either actuator or sensor or both) faults will be considered. In the fault diagnosis design, the first step is to utilize the enhanced applicability of the state observer presented in Chapter 3 to recover the full process states by using subsets of the measured outputs. To achieve robustness with respect to uncertainty, the part of the model that is used in the observer design should not be directly affected by uncertain variables. Since a maximum of two faults are considered, the observers will be designed using any $p - 1$ and $p - 2$ outputs to differentiate between the occurrence of only one or a simultaneous two faults, where p denotes the total number of outputs. The second step is to generate fault isolate residuals. The residuals sensitive to sensor faults can be generated in a similar way as in Chapter 3. The residuals sensitive to actuator faults can be generated using the differential equations such that the faults appear on the right-hand side of these equations. The third step is to design appropriate fault isolation logic that is able to differentiate between the occurrence of one actuator fault, one sensor fault, two actuator or sensor faults, and one actuator fault and one sensor fault. Since a large number of simultaneous faults would occur less frequently, the consideration of two faults would meet most of the practical needs.

Second, we consider the problem of sampled-data output feedback control using high-gain observers. The output feedback control design using high-gain observers presented in Chapter 3 assumes that the measurements of the output variables are continuously available. These results do not account for the effect of measurement sampling that arises in computer control systems, where measurements are sampled at discrete times, and the fact that certain variables (e.g., concentration and quality variables) may not be continuously available in a chemical plant. While the problem of sampled-data output feedback control using high-gain observers has been studied for nonlinear systems (see [95, 104]), the discrete nature of control implementation is not utilized to generalize the class of systems to which this type of observers can be applied. As measurement sampling is concerned, the continuous-time observer in Chapter 3 will be discretized and implemented in discrete-time as a difference equation. Two cases can be considered for sampled-data output feedback control using such observers. In the first case, the inputs are implemented to the plant at the same rate as that of measurement sampling. This case addresses a scenario where the control inputs can be prescribed at the same rate as that of measurement sampling. This can take place when an explicit control law is used, for which the computation time required by the control law may be ignored. If the computation time cannot be ignored (e.g., when MPC is used), this can take place when the control update time is sufficiently large. In the second case, measurements are sampled fast and a relatively large control update

time is used. This case addresses a scenario where the measurement sampling can be made faster than the control update rate. For example, measurements of certain variables, such as temperatures, are available at a much higher frequency than the prescription of the control inputs by MPC in a chemical plant. The use of as many measurements as possible is expected to improve the performance of state estimation and the output feedback control system.

Third, we consider the problem of safe-parking design for nonlinear process systems under output feedback control. Since the output feedback control design presented in Chapter 3 practically preserves the stability region of an equilibrium point obtained under full state feedback control, it can be used to generalize the applicability of the safe-parking approach for nonlinear process systems subject to input constraints. In particular, we consider the application of the safe-parking approach to a chemical reactor that produces polyethylene, the most widely used plastic throughout the world [124]. A gas-phase polyethylene reactor using Ziegler-Natta catalysts will be considered [125]. This process operates at an open-loop unstable equilibrium point. Because the reactor is required to operate in a relatively narrow temperature range, the reactor temperature control is extremely important to stable operation. The loss of control action due to an actuator fault may result in process instability and even lead to hazardous situations. The safe-parking approach can be used to maintain the process within a safe operating region during the period of fault repair and enable a smooth resumption of nominal operation after the fault is repaired. While the problem of safe-parking subject to limited measurements has been studied [75], the output feedback control design is subject to a restrictive structure requirement and therefore limits the scope of applications. Besides, the applicability of safe-parking has been demonstrated through a medium scale example of a styrene polymerization process [78]. However, it assumes the availability of full state measurements, which may not be the case in practice. In comparison, the proposed research will demonstrate the applicability of the safe-parking approach for a generalized class of nonlinear process systems under output feedback control through a realistic example.

References

[1] M. Morari and H. J. Lee. Model predictive control: Past, present and future. *Comp. & Chem. Eng.*, 23:667–682, 1999.

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

[3] R. Isermann and P. Balle. Trends in the application of model-based fault detection and diagnosis of technical processes. *Contr. Eng. Prac.*, 5:709–719, 1997.

[4] A. S. Willsky. A survey of design methods for failure detection in dynamic systems. *Automatica*, 12:601–611, 1976.

[5] R. Isermann. Process fault detection based on modeling and estimation methods-A survey. *Automatica*, 20:387–404, 1984.

[6] 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.

[7] P. M. Frank and X. Ding. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *J. Proc. Contr.*, 7:403–424, 1997.

[8] V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S. N. Kavuri. A review of process fault detection and diagnosis Part I: Quantitative model-based methods. *Comp. & Chem. Eng.*, 27:293–311, 2003.

[9] R. Isermann. Model-based fault-detection and diagnosis - status and applications. *Annu. Rev. Contr.*, 29:71–85, 2005.

[10] J. Bokor and Z. Szabó. Fault detection and isolation in nonlinear systems. *Annu. Rev. Contr.*, 33:113–123, 2009.

[11] R. K. Mehra and J. Peschon. An innovations approach to fault detection and diagnosis in dynamic systems. *Automatica*, 7:637–640, 1971.

[12] R. N. Clark, D. C. Fosth, and V. M. Walton. Detecting instrument malfunctions in control systems. *IEEE Trans. Aerosp. Electron. Syst.*, AES-11:465–73, 1975.

[13] R. N. Clark. Instrument fault detection. *IEEE Trans. Aerosp. Electron. Syst.*, AES-14:456–465, 1978.

[14] E. Y. Chow and A. S. Willsky. Analytical redundancy and the design of robust failure detection systems. *IEEE Trans. Automat. Contr.*, AC-29:603–614, 1984.

[15] R. J. Patton and J. Chen. Optimal unknown input distribution matrix selection in robust fault diagnosis. *Automatica*, 29:837–841, 1993.

[16] J. Chen, R. J. Patton, and H.-Y. Zhang. Design of unknown input observers and robust fault detection filters. *Int. J. Contr.*, 63:85–105, 1996.

[17] F. Hamelin and D. Sauter. Robust fault detection in uncertain dynamic systems. *Automatica*, 36:1747–1754, 2000.

[18] W. Chen and M. Saif. Adaptive actuator fault detection, isolation and accommodation in uncertain systems. *Int. J. Contr.*, 80:45–63, 2007.

[19] W. Li, S. L. Shah, and D. Xiao. Kalman filters in non-uniformly sampled multirate systems: For FDI and beyond. *Automatica*, 44:199–208, 2008.

[20] S. X. Ding, P. Zhang, A. Naik, E. L. Ding, and B. Huang. Subspace method aided data-driven design of fault detection and isolation systems. *J. Proc. Contr.*, 19:1496–1510, 2009.

[21] M. Staroswiecki and G. Comtet-Varga. Analytical redundancy relations for fault detection and isolation in algebraic dynamic systems. *Automatica*, 37:687–699, 2001.

[22] C. De Persis and A. Isidori. A geometric approach to nonlinear fault detection and isolation. *IEEE Trans. Automat. Contr.*, 46:853–865, 2001.

[23] X. Zhang, M. M. Polycarpou, and T. Parisini. A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems. *IEEE Trans. Automat. Contr.*, 47:576–593, 2002.

[24] X. Zhang, T. Parisini, and M. M. Polycarpou. Sensor bias fault isolation in a class of nonlinear systems. *IEEE Trans. Automat. Contr.*, 50:370–376, 2005.

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

[26] X. Zhang, M. M. Polycarpou, and T. Parisini. Design and analysis of a fault isolation scheme for a class of uncertain nonlinear systems. *Annu. Rev. Contr.*, 32:107–121, 2008.

[27] 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.

[28] C. W. McFall, D. Muñoz de la Peña, B. Ohran, P. D. Christofides, and J. F. Davis. Fault detection and isolation for nonlinear process systems using asynchronous measurements. *Ind. & Eng. Chem. Res.*, 47:10009–10019, 2008.

[29] X. Zhang, M. M. Polycarpou, and T. Parisini. Fault diagnosis of a class of nonlinear uncertain systems with Lipschitz nonlinearities using adaptive estimation. *Automatica*, 46:290–299, 2010.

[30] J. Liu, B. J. Ohran, D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis. Monitoring and handling of actuator faults in two-tier control systems for nonlinear processes. *Chem. Eng. Sci.*, 65:3179–3190, 2010.

[31] X. Zhang. Sensor bias fault detection and isolation in a class of nonlinear uncertain systems using adaptive estimation. *IEEE Trans. Automat. Contr.*, 56:1220–1226, 2011.

[32] Y. Hu and N. H. El-Farra. Robust fault detection and monitoring of hybrid process systems with uncertain mode transitions. *AIChE J.*, 57:2783–2794, 2011.

[33] N. H. El-Farra. Integrated fault detection and fault-tolerant control architectures for distributed processes. *Ind. & Eng. Chem. Res.*, 45:8338–8351, 2006.

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

[35] A. Armaou and M. A. Demetriou. Robust detection and accommodation of incipient component and actuator faults in nonlinear distributed processes. *AIChE J.*, 54:2651–2662, 2008.

[36] S. Ghantasala and N. H. El-Farra. Robust actuator fault isolation and management in constrained uncertain parabolic PDE systems. *Automatica*, 45:2368–2373, 2009.

[37] D. Chilin, J. Liu, D. Muñoz de la Peña, P. D. Christofides, and J. F. Davis. Detection, isolation and handling of actuator faults in distributed model predictive control systems. *J. Proc. Contr.*, 20:1059–1075, 2010.

[38] D. Chilin, J. Liu, X. Chen, and P. D. Christofides. Fault detection and isolation and fault tolerant control of a catalytic alkylation of benzene process. *Chem. Eng. Sci.*, 78:155–166, 2012.

[39] S. J. Qin. Statistical process monitoring: Basics and beyond. *J. Chemometr.*, 17:480–502, 2003.

[40] S. Mahadevan and S. L. Shah. Fault detection and diagnosis in process data using one-class support vector machines. *J. Proc. Contr.*, 19:1627–1639, 2009.

[41] S. Perk, F. Teymour, and A. Cinar. Statistical monitoring of complex chemical processes using agent-based systems. *Ind. & Eng. Chem. Res.*, 49:5080–5093, 2010.

[42] S. Perk, F. Teymour, and A. Cinar. Adaptive agent-based system for process fault diagnosis. *Ind. & Eng. Chem. Res.*, 50:9138–9155, 2011.

[43] C. F. Alcala and S. J. Qin. Analysis and generalization of fault diagnosis methods for process monitoring. *J. Proc. Contr.*, 21:322–330, 2011.

[44] V. Venkatasubramanian, R. Rengaswamy, S. N. Kavuri, and K. Yin. A review of process fault detection and diagnosis Part III: Process history based methods. *Comp. & Chem. Eng.*, 27:327–346, 2003.

[45] J. V. Kresta, J. F. MacGregor, and T. E. Marlin. Multivariate statistical monitoring of process operating performance. *Can. J. Chem. Eng.*, 69:35–47, 1991.

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

[47] H. Tong and C. M. Crowe. Detection of gross errors in data reconciliation by principal component analysis. *AIChE J.*, 41:1712–1722, 1995.

[48] S. Yoon and J. F. MacGregor. Fault diagnosis with multivariate statistical models part I: Using steady state fault signatures. *J. Proc. Contr.*, 11:387–400, 2001.

[49] S. Wold, P. Geladi, K. Esbensen, and J. Öhman. Multi-way principal components-and pls-analysis. *J. Chemometr.*, 1:41–56, 1987.

[50] W. Ku, R. H. Storer, and C. Georgakis. Disturbance detection and isolation by dynamic principal component analysis. *Chemometr. Intell. Lab. Sys.*, 30:179–196, 1995.

[51] J. Yu. A nonlinear kernel Gaussian mixture model based inferential monitoring approach for fault detection and diagnosis of chemical processes. *Chem. Eng. Sci.*, 68:506–519, 2012.

[52] M. Kano, S. Tanaka, S. Hasebe, I. Hashimoto, and H. Ohno. Monitoring independent components for fault detection. *AIChE J.*, 49:969–976, 2003.

[53] J. Wang and Q. P. He. Multivariate statistical process monitoring based on statistics pattern analysis. *Ind. & Eng. Chem. Res.*, 49:7858–7869, 2010.

[54] Q. P. He and Jin Wang. Statistics pattern analysis: A new process monitoring framework and its application to semiconductor batch processes. *AIChE J.*, 57:107–121, 2011.

[55] K. Watanabe, I. Matsuura, M. Abe, M. Kubota, and D. M. Himmelblau. Incipient fault diagnosis of chemical processes via artificial neural networks. *AIChE J.*, 35:1803–1812, 1989.

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

[57] N. Mehranbod, M. Soroush, and C. Panjapornpon. A method of sensor fault detection and identification. *J. Proc. Contr.*, 15:321–339, 2005.

[58] R. A. Martini, R. W. Chylla Jr., and A. Cinar. Fault-tolerant computer control of a time delay system: sensor failure tolerance by controller reconfiguration. *Comp. & Chem. Eng.*, 11:481–488, 1987.

[59] M. R. Basila Jr, G. Stefanek, and A. Cinar. A model-object based supervisory expert system for fault tolerant chemical reactor control. *Comp. & Chem. Eng.*, 14:551–560, 1990.

[60] R. J. Veillette. Reliable linear-quadratic state-feedback control. *Automatica*, 31:137–143, 1995.

[61] Q. Zhao and J. Jiang. Reliable state feedback control system design against actuator failures. *Automatica*, 34:1267–1272, 1998.

[62] Z. D. Wang, B. Huang, and H. Unbehauen. Robust reliable control for a class of uncertain nonlinear state-delayed systems. *Automatica*, 35:955–963, 1999.

[63] Z. D. Wang, B. Huang, and K. J. Burnham. Stochastic reliable control of a class of uncertain time-delay systems with unknown nonlinearities. *IEEE Trans. Circ. & Sys. I - Fund. Th. & App.*, 48:646–650, 2001.

[64] P. Mhaskar. Robust model predictive control design for fault-tolerant control of process systems. *Ind. & Eng. Chem. Res.*, 45:8565–8574, 2006.

[65] 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 J.*, 53:654–668, 2007.

[66] N. Kapoor and P. Daoutidis. Stabilization of nonlinear processes with input constraints. *Comp. & Chem. Eng.*, 24:9–21, 2000.

[67] 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.

[68] S. Dubljevic and N. Kazantzis. A new Lyapunov design approach for nonlinear systems based on Zubov's method. *Automatica*, 38:1999–2007, 2002.

[69] P. D. Christofides and N. H. El-Farra. *Control of Nonlinear and Hybrid Process Systems: Designs for Uncertainty, Constraints and Time-Delays*. Springer-Verlag, Berlin, Germany, 2005.

[70] N. Huynh and N. Kazantzis. Parametric optimization of digitally controlled nonlinear reactor dynamics using Zubov-like functional equations. *J. Math. Chem.*, 38:499–519, 2005.

[71] I. Karafyllis and C. Kravaris. Robust output feedback stabilization and nonlinear observer design. *Syst. & Contr. Lett.*, 54:925–938, 2005.

[72] P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Predictive control of switched nonlinear systems with scheduled mode transitions. *IEEE Trans. Automat. Contr.*, 50:1670–1680, 2005.

[73] M. Mahmood and P. Mhaskar. Enhanced stability regions for model predictive control of nonlinear process systems. *AIChE J.*, 54:1487–1498, 2008.

[74] R. Gandhi and P. Mhaskar. Safe-parking of nonlinear process systems. *Comp. & Chem. Eng.*, 32:2113–2122, 2008.

[75] M. Mahmood, R. Gandhi, and P. Mhaskar. Safe-parking of nonlinear process systems: Handling uncertainty and unavailability of measurements. *Chem. Eng. Sci.*, 63:5434–5446, 2008.

[76] R. Gandhi and P. Mhaskar. A safe-parking framework for plant-wide fault-tolerant control. *Chem. Eng. Sci.*, 64:3060–3071, 2009.

[77] M. Mahmood and P. Mhaskar. Safe-parking framework for fault-tolerant control of transport-reaction processes. *Ind. & Eng. Chem. Res.*, 49:4285–4296, 2010.

[78] R. Gandhi, D. Baldwin, and P. Mhaskar. Safe-parking of a styrene polymerization process. *Ind. & Eng. Chem. Res.*, 48:7205–7213, 2009.

[79] M. Du and P. Mhaskar. Active fault isolation of nonlinear systems. In *Proceedings of the 2012 American Control Conference*, pages 6667–6672, Montréal, Canada, 2012.

[80] M. Du and P. Mhaskar. Active fault isolation of nonlinear process systems. *AIChE J.*, provisionally accepted on August 31, 2012.

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

[82] 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. *Chem. Eng. Sci.*, 64:2370–2383, 2009.

[83] M. Du, J. Nease, and P. Mhaskar. An integrated fault diagnosis and safe-parking framework for fault-tolerant control of nonlinear systems. *Int. J. Rob. & Non. Contr.*, 22:105–122, 2012.

[84] J. P. Congalidis, J. R. Richards, and W. H. Ray. Feedforward and feedback control of a solution copolymerization reactor. *AIChE J.*, 35:891–907, 1989.

[85] M. Du, R. Gandhi, and P. Mhaskar. An integrated fault detection and isolation and safe-parking framework for networked process systems. *Ind. & Eng. Chem. Res.*, 50:5667–5679, 2011.

[86] M. Du and P. Mhaskar. A safe-parking and safe-switching framework for fault-tolerant control of switched nonlinear systems. *Int. J. Contr.*, 84:9–23, 2011.

[87] M. Du and P. Mhaskar. Isolation and handling of sensor faults in nonlinear systems. In *Proceedings of the 2012 American Control Conference*, pages 6661–6666, Montréal, Canada, 2012.

[88] M. Du and P. Mhaskar. Isolation and handling of sensor faults in nonlinear systems. *Automatica*, submitted on June 5, 2012.

[89] C. P. Tan and C. Edwards. Sliding mode observers for detection and reconstruction of sensor faults. *Automatica*, 38:1815–1821, 2002.

[90] H. Alwi, C. Edwards, and C. P. Tan. Sliding mode estimation schemes for incipient sensor faults. *Automatica*, 45:1679–1685, 2009.

[91] S. J. Qin and W. Li. Detection and identification of faulty sensors in dynamic processes. *AIChE J.*, 47:1581–1593, 2001.

[92] A. N. Atassi and H. K. Khalil. A separation principle for the stabilization of a class of nonlinear systems. *IEEE Trans. Automat. Contr.*, 44:1672–1687, 1999.

[93] N. H. El-Farra, P. Mhaskar, and P. D. Christofides. Output feedback control of switched nonlinear systems using multiple Lyapunov functions. *Syst. & Contr. Lett.*, 54:1163–1182, 2005.

[94] D. Muñoz de la Peña and P. D. Christofides. Output feedback control of nonlinear systems subject to sensor data losses. *Syst. & Contr. Lett.*, 57:631–642, 2008.

[95] J. H. Ahrens, X. Tan, and H. K. Khalil. Multirate sampled-data output feedback control with application to smart material actuated systems. *IEEE Trans. Automat. Contr.*, 54:2518–2529, 2009.

[96] R. Findeisen, L. Imsland, F. Allgöwer, and B. A. Foss. Output feedback stabilization of constrained systems with nonlinear predictive control. *Int. J. Rob. & Non. Contr.*, 13:211–227, 2003.

[97] A. T. Vemuri. Sensor bias fault diagnosis in a class of nonlinear systems. *IEEE Trans. Automat. Contr.*, 46:949–954, 2001.

[98] R. Rajamani and A. Ganguli. Sensor fault diagnostics for a class of non-linear systems using linear matrix inequalities. *Int. J. Contr.*, 77:920–930, 2004.

[99] A. M. Pertew, H. J. Marquez, and Q. Zhao. LMI-based sensor fault diagnosis for nonlinear Lipschitz systems. *Automatica*, 43:1464–1469, 2007.

[100] X. Zhang. Sensor bias fault detection and isolation in a class of nonlinear uncertain systems using adaptive estimation. *IEEE Trans. Automat. Contr.*, 56:1220–1226, 2011.

[101] X.-G. Yan and C. Edwards. Sensor fault detection and isolation for nonlinear systems based on a sliding mode observer. *Int. J. Adapt. Contr. & Sign. Process.*, 21:657–673, 2007.

[102] M. Mattei, G. Paviglianiti, and V. Scordamaglia. Nonlinear observers with H_∞ performance for sensor fault detection and isolation: a linear matrix inequality design procedure. *Contr. Eng. Prac.*, 13:1271–1281, 2005.

[103] M. Mahmood and P. Mhaskar. On constructing constrained control Lyapunov functions for linear systems. *IEEE Trans. Automat. Contr.*, 56:1136–1140, 2011.

[104] A. M. Dabroom and H. K. Khalil. Output feedback sampled-data control of nonlinear systems using high-gain observers. *IEEE Trans. Automat. Contr.*, 46:1712–1725, 2001.

[105] N. H. El-Farra and P. D. Christofides. Bounded robust control of constrained multivariable nonlinear processes. *Chem. Eng. Sci.*, 58:3025–3047, 2003.

[106] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, Upper Saddle River, NJ, 3rd edition, 2002.

[107] J. H. Ahrens and H. K. Khalil. High-gain observers in the presence of measurement noise: A switched-gain approach. *Automatica*, 45:936–943, 2009.

[108] M. Du and P. Mhaskar. Uniting safe-parking and reconfiguration-based approaches for fault-tolerant control of switched nonlinear systems. In *Proceedings of the 2010 American Control Conference*, pages 2829–2834, Baltimore, MD, 2010.

[109] Y. Lin and E. D. Sontag. A universal formula for stabilization with bounded controls. *Syst. & Contr. Lett.*, 16:393–397, 1991.

[110] S. Valluri and M. Soroush. Analytical control of SISO nonlinear processes with input constraints. *AIChE J.*, 44:116–130, 1998.

[111] P. Mhaskar, N. H. El-Farra, and P. D. Christofides. Stabilization of nonlinear systems with state and control constraints using Lyapunov-based predictive control. *Syst. & Contr. Lett.*, 55:650–659, 2006.

[112] C. Panjapornpon and M. Soroush. Shortest-prediction-horizon non-linear model-predictive control with guaranteed asymptotic stability. *Int. J. Contr.*, 80:1533–1543, 2007.

[113] M. S. Branicky, V. S. Borkar, and S. K. Mitter. A unified framework for hybrid control: model and optimal control theory. *IEEE Trans. Automat. Contr.*, 43:31–45, 1998.

[114] M. S. Branicky. Multiple Lyapunov functions and other analysis tools for switched and hybrid systems. *IEEE Trans. Automat. Contr.*, 43:475–482, 1998.

[115] J. P. Hespanha and A. S. Morse. Stability of switched systems with average dwell time. In *Proceedings of the 38th IEEE Conference on Decision and Control*, pages 2655–2660, Phoenix, AZ, 1999.

[116] I. E. Grossmann, S. A. van den Heever, and I. Harjunkoski. Discrete optimization methods and their role in the integration of planning and scheduling. In *Proceedings of the 6th International Conference on Chemical Process Control*, pages 124–152, Tucson, AZ, 2001.

[117] J. P. Hespanha and A. S. Morse. Switching between stabilizing controllers. *Automatica*, 38:1905–1917, 2004.

[118] 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. *Int. J. Adapt. Contr. & Sign. Process.*, 22:161–179, 2007.

[119] P. Daoutidis, M. Soroush, and C. Kravaris. Feedforward/feedback control of multivariable nonlinear processes. *AIChE J.*, 36:1471–1484, 1990.

[120] N. Padhiyar, S. Bhartiya, and R. D. Gudi. Optimal grade transition in polymerization reactors: A comparative case study. *Ind. & Eng. Chem. Res.*, 45:3583–3592, 2006.

[121] M. Du, R. Gandhi, and P. Mhaskar. Fault detection and isolation and safe-parking of networked systems. In *Proceedings of the 2011 American Control Conference*, pages 3146–3151, San Francisco, CA, 2011.

[122] E. Tatara, I. Birol, F. Teymour, and A. Cinar. Agent-based control of autocatalytic replicators in networks of reactors. *Comp. & Chem. Eng.*, 29:807–815, 2005.

[123] J. Liu, D. Muñoz de la Peña, and P. D. Christofides. Distributed model predictive control of nonlinear process systems. *AIChE J.*, 55:1171–1184, 2009.

[124] E. Benham and M. McDaniel. *Kirk-Othmer Encyclopedia of Chemical Technology*. John Wiley & Sons, Inc., 2000.

[125] A. Gani, P. Mhaskar, and P. D. Christofides. Fault-tolerant control of a polyethylene reactor. *J. Proc. Contr.*, 17:439–451, 2007.

Appendix A

Proofs

A.1 Proof of Theorem 4.2

Consider three possibilities:

Case 1. No fault takes place. The absence of faults implies $u(t) = u_{nom,\sigma(t)}(t)\ \forall\, t \in [0, t_l]$. Since $x(0) \in \Omega_{nom,\sigma(0)}$ and Assumption 4.1 holds, it follows from Section 4.2.2 that $x(t) \in \Omega_{nom,\sigma(t)}\ \forall\, t \in [0, t_l]$ and $\|x(t_i) - x_{nom,k_i}\| \leq d\ \forall\, i \in \{1, \ldots, l\}$, with $\mathcal{B} = \varnothing$.

Case 2. A fault is detected and isolated at time t_d, and it is repaired at time t_r, with $t_s < t_l$ (nominal operation is resumed). Recall that FDI takes place in mode k_a and the fault is repaired in mode k_b. We prove for the case when $b > a$ (i.e., FDI and fault repair occur in different modes), while the proof for the case when $b = a$ (i.e., FDI and fault repair occur in the same mode) follows from a similar line of arguments. We first show that the system can be safe-parked in mode k_a. Note that $u(t) = u_{s,k_a}(t)\ \forall\, t \in [t_d, t_a)$. Since $x(t_d) \in \Omega_{s,k_a} \subseteq \Omega_{nom,k_a}$ and $T_f \leq t_a - t_d$, it follows from Section 4.2.2 that $x(t) \in \Omega_{nom,k_a}\ \forall\, t \in [t_d, t_a)$ and $x(t_a) \in B_{d,s,k_a}$. Next, we show that the system can be safe-parked successively and nominal operation can be resumed at time t_s. Note that $u(t) = u_{s,\sigma(t)}(t)$ $\forall\, t \in [t_a, t_s)$. Since $x(t_a) \in B_{d,s,k_a}$, $B_{d,s,k_i} \subseteq \Omega_{s,k_{i+1}} \subseteq \Omega_{nom,k_{i+1}}$, and $T^s_{k_i,k_{i+1}} \leq t_{i+1} - t_i$ $\forall\, i \in \{a, \ldots, l-1\}$, we have from Section 4.2.2 that $x(t) \in \Omega_{nom,\sigma(t)}\ \forall\, t \in [t_a, t_s)$, $x(t_s) \in \Omega_{nom,k_b}$ if $T_r \leq t_b - t_r$, and $x(t_s) \in \Omega_{nom,k_{j+1}}$ if $T_r > t_b - t_r$. Thus, the rest of the proof follows from Case 1 when the system operates in mode $k_i\ \forall\, i \in \{1, \ldots, a_0\} \cup \mathcal{B}$, where $\mathcal{B} = \{b, \ldots, l\}$ if $T_r \leq t_b - t_r$ and $\mathcal{B} = \{j+1, \ldots, l\}$ if $T_r > t_b - t_r$, with nominal control action $u(t) = u_{nom,\sigma(t)}(t)\ \forall\, t \in [0, t_f] \cup [t_s, t_l]$.

Case 3. A fault is detected and isolated at time t_d, and it is repaired at time t_r, with $t_s = t_l$ (i.e., nominal operation is not resumed; see Remark 4.8 for an explanation). It follows from Case 2 that $x(t) \in \Omega_{nom,\sigma(t)} \; \forall \; t \in [0, t_f] \cup [t_d, t_l]$ and $\|x(t_i) - x_{nom,k_i}\| \leq d \; \forall \; i \in \{1, \ldots, a_0 - 1\}$, with $\mathcal{B} = \varnothing$.

In conclusion, $x(t) \in \Omega_{nom,\sigma(t)} \; \forall \; t \in [0, t_f] \cup [t_d, t_l]$ and $\|x(t_i) - x_{nom,k_i}\| \leq d \; \forall \; i \in \{1, \ldots, a_0 - 1\} \cup \mathcal{B}$. This completes the proof of Theorem 4.2. □

A.2 Proof of Theorem 4.3

Consider two possibilities:

Case 1. No fault takes place. The proof is the same as that of Theorem 4.2.

Case 2. A fault is detected and isolated at time t_d, and it is repaired at time t_r. We first show that the system state can be driven to enter the stability region $\hat{\Omega}_{k_c}$ under the control law to safe-park in mode k_a. Note that $u(t) = u_{s,k_a}(t) \; \forall \; t \in [t_d, t'_a)$. Since $x(t_d) \in \Omega_{s,k_a} \subseteq \Omega_{nom,k_a}$ and $B_{d,s,k_a} \subseteq \hat{\Omega}_{k_c}$, it follows from Section 4.2.2 that $x(t) \in \Omega_{nom,k_a} \; \forall \; t \in [t_d, t'_a)$, and there exists a finite time t'_a such that $x(t'_a) \in \hat{\Omega}_{k_c}$. Next, we show that the system can be stabilized at the nominal equilibrium point for mode k_c. Note that $u(t) = \hat{u}_{k_c}(t)$ $\forall \; t \in [t'_a, t'_c)$. Since $x(t'_a) \in \hat{\Omega}_{k_c}$ and $t'_c \geq t'_a + T_c$, it follows from Section 4.2.2 that $x(t) \in \hat{\Omega}_{k_c} \subseteq \Omega_{nom,k_c} \; \forall \; t \in [t'_a, t'_c)$ and $x(t'_c) \in \Omega_{nom,k_{c+1}}$. Since $t'_c \geq t_r$ and $x(t'_c) \in \Omega_{nom,k_{c+1}}$, the rest of the proof follows from Case 1 when the system operates in mode $k_i \; \forall$ $i \in \{1, \ldots, a_0\} \cup \{c + 1, \ldots, l\}$, with the nominal control action $u(t) = u_{nom,\sigma(t)}(t) \; \forall$ $t \in [0, t_f]$ or $u(t) = u_{nom,\sigma'(t)}(t) \; \forall \; t \in [t'_c, t'_l]$.

In conclusion, $x(t) \in \Omega_{nom,\sigma(t)} \; \forall \; t \in [0, t_f]$, $\|x(t_i) - x_{nom,k_i}\| \leq d \; \forall \; i \in \{1, \ldots, a_0 - 1\}$, $x(t) \in \Omega_{nom,\sigma'(t)} \; \forall \; t \in [t_d, t'_l]$, and $\|x(t'_i) - x_{nom,k_i}\| \leq d \; \forall \; i \in \{c, \ldots, l\}$. This completes the proof of Theorem 4.3. □