Universitat Politècnica de Catalunya

Programa de Doctorat:

Automàtica, Robòtica i Visió

Tesi Doctoral

DIAGNOSIS AND FAULT-TOLERANT CONTROL USING SET-BASED METHODS

Feng XU

Directors: Dr. Vicenç Puig Cayuela i Dr. Carlos Ocampo Martínez

Setembre de 2014

To my family and people who encourage me. . .

"Only knowledge is eternal !"

Declaration

I hereby declare that this dissertation is the result of my own work and is not substantially the same as any work that has been submitted for a degree, diploma or other qualifications at any other university or institution.

Feng XU

Barcelona, Spain, September 2014

Acknowledgements

It is an exciting moment for me to arrive at the end of my Ph.D. research. On the road to this moment, like most of Ph.D. students, I have experienced excitement, depression, success and failure. But, nowadays all of these complex feelings have been integrated into my life of this period, which has added beautiful colors to my memory. The past time of my Ph.D. research has significant impact on my mind, knowledge, value, etc. Thanks to this period, I have built a foundation for my future academic exploration. Wherever I will be, I will try my best to use the knowledge and experience I have obtained to contribute to the world, my country, my family and myself. Here, I want to express my sincerest gratitude to those people/institutions deeply affecting me during this wonderful journey.

First, I want to thank my Ph.D. supervisors Dr. Vicenç Puig Cayuela and Dr. Carlos Ocampo Martínez for their efforts to guide me. They help me a lot from the application of my Ph.D. position to my daily life in Barcelona. I recall that, especially at the beginning, I almost know nothing about the city, the university, the institute and the research topic. However, they guide me to learn how to find materials, propose ideas, write scientific documents and so on with their great patience. They also establish academic platforms to let me share ideas with some other researchers in the field, which is key for me to understand the world of knowledge. If I become a researcher/teacher in the future, these experience will be my wealth.

Second, I want to thank Dr. Sorin Olaru from Supelec (France). In my eyes, he is an excellent researcher who can always give me some key suggestions from writing to thinking. Sometimes, he "attacks" my ideas and gives harsh comments. But because of these rigid suggestions, I can be driven to do something better than what I imagine at the beginning. This is very helpful for me to grow up. Besides, I also thank Dr. Sorin Olaru and Dr. Silviu-Iulian Niculescu to accept me as a visiting Ph.D. student in Supelec and finance my academic stay there. This experience gives me chance to understand how the people in one of the most prestigious French schools are doing their research. With no doubt, I am inspired by the people there. Hence, I want to express my gratitude to all the people (Didier Dumur, Pedro Rodriguez, Martin Gulan, Ngoc Anh Nguyen, Minh Tri Nguyen, Mohamad Koteich, Sofiane Ben Chabane, etc.) I met in the Automatic Control Group of Supelec for their help.

Third, I want to thank Dr. Florin Stoican from the “Politehnica” University of Bucharest (Romania) for his help on the topic of invariant sets in fault detection and isolation and fault-tolerant control. Frankly speaking, I learn about my Ph.D. topic by starting reading his wonderful Ph.D. dissertation. In my research, whenever I meet some troubles on the topic and send emails to him for help, he always patiently gives me constructive suggestions to continue my work. He also gives me a lot of important comments for my research papers and helps me improve my writing skills.

Fourth, I want to thank all the people (Juan Manual Grosso Pérez, Bernat Joseph Duran, Syed Farzad Husain, David Martínez Martínez, Eloy Retamino Carrion, Edgar Simo Serra, etc.) at the Institut de Robòtica i Informàtica Industrial. They provide me a friendly atmosphere, which allows me to focus on my research and enjoy my life in Barcelona. Especially

thank Juan Manual Grosso Pérez who always positively discusses some common topics of our research with me and motivates me a lot. I will always memorize the precious lunch time together with these inspiring people.

Fifth, I want to thank my undergraduate supervisor Dr. Jiang Dongfang in the School of Automation of the Northwestern Polytechnical University, Xi'an, P.R.China. He guides me from a childish middle school student to an engineer. Not only before but also after I left the university, I have been obtaining important suggestions from him to plan my future career.

Sixth, I want to thank my Ph.D. Scholarship provider (China Scholarship Council). This is an organization that takes responsibility for the Chinese government to select and finance thousands of excellent Chinese master and Ph.D. students every year to pursue higher academic experience in world-famous universities/institutes. For the government, the council and the students, I believe that we have a common dream to completely revive the historical glory of the country as one of the most important leaders in the world. Based on the current economic, scientific and technical foundations built by the previous generations, I always believe that our young generation can completely accomplish this historical mission.

Seventh, I want to thank the projects/grants that partially finance my research. They are the Spanish research projects CICYT SHERECS DPI-2011-26243 and WATMAN (DPI2009-13744) of the Science and Technology Ministry, the DGR of Generalitat de Catalunya (SAC group Ref. 2009/SGR/1491) and the contract i-Sense (FP7-ICT-2009-6-270428) by the European Commission.

Finally, I want to thank my parents, brother, relatives and friends who encourage me. Especially for my parents, I only went back to see them one time during my Ph.D. because of time. Hence, I always feel guilty that I do not take enough responsibility to observe filial piety.

Feng XU

Barcelona, Spain, September 2014

Abstract

The fault-tolerant capability is an important performance specification for technical systems. Examples showing its importance are some catastrophes in civil aviation. According to official investigations, some air accidents due to failures are technically avoidable if the pilots can take right measures. But, relying on the skill and experience of the pilots, it cannot be guaranteed that reliable flight decisions are always made. Instead, if fault-tolerant strategies can be included in the decision-making procedure, it will be very useful for safer flight.

Fault-tolerant control is generally classified into passive and active fault-tolerant control. Passive fault-tolerant control relies on the robustness of the controller, which can only provide limited fault-tolerant ability, while active fault-tolerant control turns to a fault detection and isolation module to obtain fault information and then to actively take actions to tolerate the effect of faults. Generally, active fault-tolerant control has more powerful fault-tolerant ability than passive fault-tolerant control.

In this dissertation, one focuses on active fault-tolerant control, which for this case considers model predictive control and set-based fault detection and isolation. Model predictive control is a successful advanced control strategy in process industry and has been widely used for processes such as chemistry and water treatment, because of its ability to deal with multivariable constrained systems. However, the performance of model predictive control has deep dependence on model accuracy. Realistically, it is impossible to avoid the effect of modelling errors, disturbances, noises and faults, which always result in model mismatch. Comparatively, model mismatch induced by faults is possible to be effectively handled by suitable fault-tolerant strategies. The objective of this dissertation is to endow model predictive control with fault-tolerant ability to improve its effectiveness. In order to reach this objective, set-based fault detection and isolation methods are used in the proposed fault-tolerant schemes. The important advantage of set-based fault detection and isolation is that it can make robust fault detection and isolation decisions, which is the key for taking right fault-tolerant measures.

This dissertation includes four parts. The first part introduces this research, presents the state of the art and gives an introduction of used research tools. The second part proposes set-based fault detection and isolation for actuator and sensor faults, which is involved in interval observers and invariant sets. In the second part, the relationship between interval observers and invariant sets is firstly investigated. Then, actuator and sensor faults are separately coped with depending on their own features. The third part focuses on actuator and sensor fault-tolerant model predictive control, where the control strategy is robust model predictive control. The last part draws some conclusions, summarizes this research and gives clues for the future work.

Key words: Fault Detection and Isolation, Fault-tolerant Control, Model Predictive Control, Invariant Sets, Interval Observers, Zonotopes.

摘要

容错能力对于大多数技术系统而言是一项重要的性能指标。 能够充分说明这一点的例子是近些年部分因故障而发生的空难。根据他们的官方调查报告， 如果事发时飞行员能够采取正确的方式操纵飞机，那么一些由故障引起的空难从技术的角度上是可以避免的。 尽管如此，想要完全依靠飞行员的飞行技术及经验来避免类似事故也是相当不可靠的。 在这种情况下，假如能将容错控制的方法和思想包含在整个飞行决策过程中，那么飞行安全性在一定程度上可以提高。

通常情况下，容错控制被分为两个大类，即被动容错控制和主动容错控制。 被动容错控制的实现主要依靠控制器自身的鲁棒性能，因此这种容错控制策略的容错能力有限，并且随着考虑的故障类型增多而性能降低。 不同于被动容错控制，主动容错控制包含一个故障检测与诊断模块。这个模块的功能在于检测故障并获取故障相关信息。 一旦故障信息被有效获取，这些信息便可以被用于容错决策的产生过程。这样，系统便可以主动地采取适当措施来容忍这些故障所带来的影响。 因此，一般来说，主动容错控制会有更多灵活性，容错能力也相对更强。 本文主要关注的是主动容错控制，其中本文研究所涉及的领域包括鲁棒模型预测控制、集基于的故障诊断。

模型预测控制是一种已成功应用于过程工业的高级控制策略，例如化工和水处理过程的控制问题。其主要特点在于它能有效处理约束多变量系统的控制问题。 这一点对于其他现存的控制策略而言是相对更具挑战的。虽然如此，但模型预测控制的性能对被控系统的模型准确度有较高的要求，如果实际系统与所用模型之间存在较大误差，那么控制系统的性能也可能出现大的偏差。在实际情况中，模型不匹配可由多种因素导致，包括扰动、噪声、建模误差，故障等。 这些因素中，其中故障所导致的模型不匹配是最具有风险的。尽管如此，相对于其他模型不匹配因素而言，故障也是最可能通过适当的容错控制策略进行有效处理的。 因此，本文的目标主要是赋予模型预测控制以容错能力，来提高它在实际应用中的有效性，以期更好地发挥其相对于其他控制策略的优势。 为了达到这一目标，本研究采用了集基于的故障检测与隔离方法，用以获得故障检测与隔离的鲁棒性。这一点也往往对于容错控制非常关键。

本论文被分为四个部分。第一部分主要介绍所做的研究，研究课题的概况及其最新进展，并且对该研究所涉及到的具体方法进行了介绍。第二部分分别提出了适用于执行器和传感器的集基于的故障检测与隔离方法。 主要涉及到间隔观测器和不变集。其中，首先研究了间隔观测器和不变集两种集基于的方法在故障诊断应用上的联系，然后根据这些调查结果分别提出了新的执行器和传感器故障检测与隔离方法。 第三部分，主要是基于第二部分提出的故障检测和隔离方法来进一步考虑执行器和传感器的容错控制问题。其中，所采用的的控制策略是鲁棒模型预测控制。 最后一部分主要是针对本论文的研究结果给出了一些相关结论，进行总结并且对未来该方向的研究进行展望。

关键词: 故障检测与隔离、容错控制、模型预测控制、间隔观测器、不变集、环带多面体。

Resumen

La capacidad de los sistemas para tolerar fallos es una importante especificación de desempeño para la mayoría de sistemas. Ejemplos que muestran su importancia son algunas catástrofes en aviación civil. De acuerdo a investigaciones oficiales, algunos incidentes aéreos son técnicamente evitables si los pilotos pudiesen tomar las medidas adecuadas. Aun así, basándose en las habilidades y experiencia de los pilotos, no se puede garantizar que decisiones de vuelo confiables serán siempre posible de tomar. En cambio, si estrategias de tolerancia a fallos se pudieran incluir en el proceso de toma de decisión, los vuelos serían mucho más seguros.

El control tolerante a fallos es generalmente clasificado en control pasivo y activo. El control pasivo se basa en la robustez del controlador, el cual sólo provee una habilidad limitada de tolerancia a fallos, mientras que el control tolerante a fallos de tipo activo se convierte en un modulo de detección y aislamiento de fallos que permite obtener información de éstos, y luego, activamente, tomar acciones para tolerar el efecto de dichos fallos. Así pues, el control activo generalmente tiene habilidades más fuertes de tolerancia a fallos.

Esta tesis se enfoca en control tolerante a fallos activo, para lo cual considera el control predictivo basado en modelos y la detección y aislamiento de fallos basados en conjuntos. El control predictivo basado en modelos es una estrategia de control exitosa en la industria de procesos y ha sido ampliamente utilizada para procesos químicos y tratamiento de aguas, debido a su habilidad de tratar con sistemas multivariables con restricciones. A pesar de esto, el desempeño del control predictivo basado en modelos tiene una profunda dependencia de la precisión del modelo del sistema. Siendo realistas, es imposible evitar el efecto de errores de modelado, perturbaciones, ruidos y fallos, que siempre llevan a diferencias entre el modelo y el sistema real. Comparativamente, el error de modelo inducido por los fallos es posible de ser manejado efectivamente por estrategias adecuadas de control tolerante a fallos. Con el fin de alcanzar este objetivo, métodos de detección y aislamiento de fallos basados en conjuntos son utilizados en los esquemas de tolerancia a fallos propuestos en esta tesis. La ventaja importante de estas técnicas de detección y aislamiento de fallos basadas en conjuntos es que puede tomar decisiones robustas de detección y aislamiento, lo cual es clave para tomar medidas acertadas de tolerancia a fallos.

Esta tesis esta dividida en cuatro partes. La primera parte es introductoria, presenta el estado del arte y hace una introducción a las herramientas de investigación utilizadas. La segunda parte expone la detección y aislamiento de fallos en actuadores y/o sensores, basándose en teoría de conjuntos, a partir de observadores de intervalo, y conjuntos invariantes. La tercera parte se enfoca en el control predictivo robusto (con enfoques basados tanto en tubos robustos como en min-max) con tolerancia a fallos en actuadores y/o sensores. La cuarta parte presenta algunas conclusiones, hace un resume de esta investigación y da algunas ideas para trabajos futuros.

Palabras clave: Detección y Aislamiento de Fallos, Control Tolerante a Fallos, Control Predictivo Basado en Modelos, Conjuntos Invariantes, Observadores de Intervalos, Zonotopes.

Vitae

Feng XU was born on January 04, 1988 (or November 15, 1987 in lunar calender), in Tianmen, Hubei, P.R. China. He received his bachelor's degree in Measurement and Control Technology & Instruments from the School of Automation of the Northwestern Polytechnical University (NWPU), Xi'an, Shaanxi, P.R.China, in July 2010. From September 2010 to July 2011, he was a master student in Control Theory & Control Engineering in the same school. From October 2011 to October 2014, he was a Ph.D. candidate in Automatic Control at the Institut de Robòtica i Informàtica Industrial (CSIC-UPC), Technical University of Catalonia (UPC), Barcelona, Catalonia, Spain.

Contents

Notations

$\mathbb{B}^r$	Unitary box composed of r unitary intervals
$\mathbb{R}$	Set of real numbers
$\mathbb{R}_+$	Set of positively real numbers
$\mathbb{R}^n$	Set of n-dimensional real vectors
$\mathbb{R}^n_+$	Set of n-dimensional positively real vectors
$\mathbb{R}^{m\times n}$	Set of real $m \times n$ matrices
$\mathbb{N}$	Set of natural numbers
$\lvert\cdot\rvert$	Absolute value
$\lVert\cdot\rVert_s$	Euclidean s-norm
$\oplus$	Minkowski sum
$\ominus$	Pontryagin difference
I	Identity matrix with suitable dimensions
O	Zero matrix with suitable dimensions
$\mathrm{diag}(\cdot)$	Diagonal matrix with suitable dimensions
$\mathrm{center}(\cdot)$	Center of a centered set
α^T	Transpose of a vector/matrix α
$[\underline{x}, \overline{x}]/(\underline{x}, \overline{x})$	Interval/Open interval
$(x_1, x_2, \ldots, x_n)$	Row vector
$([\underline{x}_1, \overline{x}_1], [\underline{x}_2, \overline{x}_2], \ldots, [\underline{x}_n, \overline{x}_n])$	Row interval vector

Acronyms

FTC	Fault-tolerant Control
AFTC	Active Fault-tolerant Control
PFTC	Passive Fault-tolerant Control
FD	Fault Detection
FI	Fault Isolation
FDI	Fault Detection and Isolation
FDD	Fault Detection and Diagnosis
MPC	Model Predictive Control
FTMPC	Fault-tolerant Model Predictive Control
PI	Positively Invariant
RPI	Robust Positively Invariant
mRPI	Minimal Robust Positively Invariant
CI	Controlled Invariant
MCI	Maximal Controlled Invariant
RCI	Robust Controlled Invariant
MRCI	Maximal Robust Controlled Invariant

List of Figures

List of Tables

Part I

Preliminaries

Chapter 1

Introduction

This chapter states the motivation, objectives and state of the art of the research area this dissertation is contributing to, which will be separately detailed in different sections of this dissertation. Additionally, a brief outline of this dissertation is also presented, which introduces the contents and contributions of each chapter.

1.1 Motivation

As the technical systems become more and more sophisticated, their sensitivity to the effect of faults increases considerably. Generally, the occurrence of faults always affects the system performance to some extent. In the severe case, the system even fails and results in catastrophes. This implies that it is necessary to take measures for avoidance of the possible aftermath induced by faults [5, 6].

The technique to reduce/eliminate the effect of faults in controlled systems is named as FTC, whose implementation is generally classified into two steps, i.e., FDD and control redesign. The objective of FDD is to detect, isolate, identify and estimate faults after they have affected the system behaviors. Fault detection determines whether a fault has occurred or not in a system, fault isolation finds the system component where the fault has occurred and fault identification and estimation determine the fault type and magnitude. By FDD, some important fault information can be obtained on-line, which will be used as the references of control redesign to take measures for achieving fault tolerance. In this dissertation, the focus of FDD is FDI while fault identification and estimation are not considered. However, the readers can see [5] for more relevant knowledge on this topic. Then, after obtaining the fault information from the FDD module, the next step is to tolerate the effect of faults based on proper control techniques. The expected objective of FTC is to guarantee that the faulty system can still achieve satisfactory performance and avoid failure in the presence of faults. However, a degree of degradation is allowed in some faulty situations, as long as the safety

of the system can be guaranteed.

The final goal of this dissertation is to design FTC schemes based on set-based FDI and model predictive control. Thus, the statement of this dissertation is divided into two parts, i.e., FDI and FTC. The advantage of set-based FDI is that it can provide FDI robustness to cope with the effect of uncertainties (parametric uncertainties, process disturbances, measurement noises, biases, etc.) on the reliability of FDI decisions [19, 20, 48]. The set-based FDI techniques used in this dissertation are mainly involved in invariant sets and interval observers. Generally, invariant sets are used to describe the steady-state behaviors of the system dynamics and interval observers can monitor the dynamic behaviors of the system during the whole dynamic process [2, 3, 18, 26, 27, 53]. In the FDI part of this dissertation, the motivation is mainly from the strengths of invariant sets and interval observers at transient and steady states, respectively. First, interval observers can monitor the whole dynamic process while invariant sets only describe the steady-state behaviors of the system. Second, by using invariant sets to establish FDI conditions at steady state, interval observers perhaps can be extended from FD to FI applications without needing help of other FI techniques such as the fault signature matrix methods [7, 47]. Empirically, if one can combine invariant sets and interval observers, it is possible to find new methods to mitigate the disadvantages and exert the advantages of each other and to obtain more efficient robust FDI techniques. The details will be given throughout the dissertation.

Model predictive control, considered in this dissertation as the control strategy, is an important topic in the control field, which has attracted a considerable number of researchers to devote themselves to its development [8, 12, 32]. The advantages of MPC are that it can effectively deal with the multivariable constrained system and simultaneously generate the optimal control actions, which are difficult for other control strategies. Hence, it is strongly motivated to develop fault-tolerant capability for MPC, which will be meaningful from practical point of view [31]. However, as the name *model predictive control* indicates, it is known that the performance of an MPC controller-based system deeply depends on the accuracy of its system model. If the system model has obvious mismatch with the real system, satisfactory system performance may not be able to be achieved. In reality, this model mismatch may be due to uncertainties and faults. As one of the important factors of model mismatch, it is known that faults imply changes of system models. Thus, if an FDD mechanism can be smoothly incorporated into the MPC controller-based system, the model mismatch induced by faults can be considerably reduced by using the obtained fault information to take fault-tolerant measures. This is an important motivation of this research.

In this dissertation, the system uncertainties such as process disturbances and measurement noises are taken into account. In this case, the results of this research can be more connected to the reality. However, due to the system uncertainties, both FDI and control should be robust to the effect of the uncertainties. Otherwise, the final performance may not be satisfactory. This motivates the use of robust FDI and robust

MPC [28, 35]. By combining set-based robust FDI and robust MPC, this research has more important significance for fault tolerance of the multivariable constrained system with uncertainties. Additionally, in reality, different types of faults may occur in a controlled system such as faults in the plant, actuators and sensors. In general, the faults in actuators and sensors are more probable to occur and affect the system performance, which draws considerable attention of the researchers. Thus, this dissertation focuses on actuator and sensor faults. But theoretically, the proposed approaches in this dissertation should also be able to be extended for faults in the plant. However, this extension needs rigorous mathematical proofs, which could be considered as a work in the future. Currently, this dissertation only concentrates on detection, isolation and tolerance of actuator and sensor faults.

1.2 Objectives of Dissertation

The overall objective of this dissertation is to implement fault-tolerant predictive control using set-based methods for achieving actuator/sensor fault tolerance. In order to reach it, this overall objective is divided into several stage objectives.

- Objective 1 : Compare invariant sets with interval observers in FD and summarize their advantages and disadvantages with respect to each other.
- Objective 2 : Combine invariant sets with interval observers to extend the applications of interval observers from FD to FI.
- Objective 3 : Integrate set-based FDI and robust MPC to obtain actuator/sensor FTMPC schemes.

Objective 1 is the basis of the entire research in this dissertation. In order to implement FTMPC schemes, it is necessary to develop efficient FDI methods. The expected scheme should have robustness, which motivates the use of the set-based FDI methods. Thus, the first step is to compare the existing set-based FDI approaches including those based on invariant sets and interval observers. The invariant set-based FDI approach requires the separation of invariant sets, where each invariant set corresponds to one considered system mode (healthy or faulty). Since invariant sets describe the steady-state system behaviors, the detection and isolation of faults using invariant sets reduce to test in which invariant set (healthy or faulty) the residual signal[1] is at steady state. Differently, interval observers can monitor the dynamic behaviors of the system during the whole process. Thus, the interval observer-based method can detect faults even at transient state. This motivates to investigate the two FD approaches, explore their advantages and disadvantages and find possibilities to combine them to obtain better FDI performance.

[1]The residual is a signal that is sensitive to faults and with a manageable dependence on disturbances.

Objective 2 follows Objective 1. In the literature [20, 39], interval observers are successfully used in FD but not FI. Generally, FDI approaches based on interval observers rely on other FI techniques to implement FI [7, 47]. Objective 2 is to use invariant sets as a tool to implement the interval observer-based FI. In this way, interval observers can independently implement both FD and FI and simultaneously obtain robust state estimation, which is good for both FDI and control design of FTC schemes. Since faults in actuators and sensors have different characteristics, if one wants to obtain FDI guarantees as less conservative as possible, actuator and sensor FDI are generally considered, separately. Thus, actuator and sensor FDI algorithms are implemented under this objective, respectively.

Objective 3 aims at implementing FTMPC schemes for actuator and sensor faults. In Objective 2, only the set-based detection and isolation of faults are done while the tolerance of faults are not considered. Thus, FTC is the main task of Objective 3. Generally, feedback control strategies are used in control of fault-tolerant control schemes. However, feedback control strategies only have limited ability especially when considering the system with constraints. Thus, in the proposed FTC schemes, MPC is chosen as the control strategy. Additionally, other issues like state estimation for MPC controllers, stability and feasibility should also be taken into account.

1.3 Outline of Dissertation

This dissertation aims to combine several existing set-based FDI methods to obtain more efficient set-based FDI approaches for detection and isolation of actuator/sensor faults. At the first step, new set-based FDI approaches are proposed. Under the proposed FDI framework, different measures are further considered to improve the set-based FDI approaches. At the second step, FTC based on MPC is introduced to this framework. Thus, some measures to integrate FTC with FDI are taken to assure the normal operation of MPC controllers and further improve the proposed set-based FDI approaches by impacting the effect of control actions on the closed-loop systems. The remainder of this dissertation is organized as follows:

- **Chapter** 2 introduces research tools, which are mainly involved in set theory and MPC. Notice that this chapter is the pavement for the rest of the dissertation. For more details about the use of these tools in the proposed FTC schemes, one should read the relevant contents of this dissertation.
- **Chapter** 3 analyzes and compares two set-based FD approaches, i.e., invariant set-based and interval observer-based. According to the results, both approaches have advantages and disadvantages. The relationship of these two approaches are briefly investigated, which is the basis of the proposed set-based approaches. This chapter is based on the publication:

F. Xu, F. Stoican, V. Puig, C. Ocampo-Martinez, and S. Olaru. On the relationship between interval observers and invariant sets in fault detection. In Proceedings of the 2nd International Conference on Control and Fault-Tolerant Systems, October 9-11 2013, Nice, France.

- **Chapter** 4 proposes an actuator FDI approach based on interval observers and invariant sets. The proposed approach simultaneously includes two different FI mechanisms, i.e., transient-state FI with need of more computational resources and steady-state FI with need of more FI time. Thus, the proposed approach is flexible enough. But the particular selection of FI mechanisms should be determined according to the applications. This chapter is based on the publications:

  F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Actuator Fault Detection and Isolation based on Invariant Sets and Interval Observers. In proceedings of the 52nd IEEE Conference on Decision and Control, December 10-13, 2013, Florence, Italy.

  F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Actuator-fault Detection and Isolation based on Set-theoretic Approaches. Journal of Process Control, 24(6), 947-956, 2014.

- **Chapter** 5 proposes a sensor FDI approach by making full use of the system-operating information from all interval observers, which is based on interval observers and invariant sets and establishes a collection of invariant set-based guaranteed FDI conditions. This chapter is based on the publications:

  F. Xu, F. Stoican, V. Puig, C. Ocampo-Martinez, and S. Olaru. Fault detection and isolation based on the combination of a bank of interval observers and invariant sets. In proceedings of the 21st Mediterranean Conference on Control and Automation, June, 2013, Chania, Greece.

  F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Improved Fault Detection and Isolation Strategy using a Bank of Interval Observers. In proceedings of 2014 IFAC World Congress, August 24-29, 2014, Cape Town, South Africa.

  F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Set-theoretic Methods in Robust Detection and Isolation of Sensor Faults. Submitted to International Journal of Systems Science.

- **Chapter** 6 proposes an actuator FTMPC scheme using the output feedback robust MPC technique. In the proposed FTC scheme, FDI is implemented by using the conventional observers, which means that both FTC and FDI techniques used in the proposed scheme have relatively low complexity. This is the advantage of this FTMPC scheme. This chapter is based on the publications:

  F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Closed-loop Actuator-fault Detection and Isolation using Invariant Sets and Tubes. In

proceedings of 2014 IFAC World Congress, August 24-29, 2014, Cape Town, South Africa.

F. Xu, V. Puig, C. Ocampo-Martinez, S. Olaru and S. Niculescu. Robust MPC for Actuator-fault Tolerance using Set-based Passive Fault Detection and Active Fault Isolation. Accepted to the 53rd IEEE Conference on Decision and Control, December 15-17, 2014, Los Angeles, CA, USA.

- **Chapter** 7 implements an FTMPC scheme for sensor faults. The contribution of this chapter consists in proposing an active FI strategy based on robust MPC for sensor FTC. This scheme has less conservative FI conditions than the passive fault diagnosis methods and decouples the effect of sensor faults on different system output components in terms of FI. In this way, the isolation of sensor faults can be simplified. This chapter is based on the publications:

  F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Sensor-fault Detection and Isolation using Interval Observers. In proceedings of the 2nd International Conference on Control and Fault-Tolerant Systems, October 9-11, 2013, Nice, France.

  F. Xu, S. Olaru, V. Puig, C. Ocampo-Martinez and S. Niculescu. Sensor-fault Tolerance using Robust MPC with Set-based State Estimation and Active Fault Isolation. Accepted to the 53rd IEEE Conference on Decision and Control, December 15-17, 2014, Los Angeles, CA, USA.

- **Chapter** 8 summarizes the whole research presented in this dissertation, foresees the development of the related topics of this dissertation and gives some clues for the future research.

Chapter 2

Research Background

This chapter introduces the background knowledge related to this research, which includes polyhedral sets, invariant sets and robust MPC. The set-theoretic methods are the core tools of FDI of this research. The robust MPC technique is the control strategy used for fault tolerance in the proposed FTC schemes.

2.1 State of the Art

This section introduces the notions of faults and fault tolerance and briefly reviews the progress of fault-tolerant strategies. Considering that the topic of this dissertation concentrates on fault tolerance using robust MPC and set-theoretic methods, this section focuses on the research background related to these areas.

2.1.1 Faults and Fault Tolerance

A fault in a dynamic system is a deviation of the system structure or system parameters from its nominal system [5]. Faults may occur in the plant, sensors or actuators. Plant faults change the plant input/output relationship, sensor faults affect the link of the plant and controller, while actuator faults reduce the ability of the controller to influence the plant. Generally, the occurrence of faults always affects the normal operation of the system to some extent, seriously even resulting in catastrophes. For the sake of preserving system performance, failure avoidance/system safety, some necessary measures should be taken for the fault-affected system.

The objective of FTC is to keep the system performance even in the presence of faults. Generally, FTC is classified into passive fault-tolerant control (PFTC) and active fault-tolerant control (AFTC) [5]. PFTC utilizes the controller robustness to tolerate the effect of faults, where one robust controller is used to resist the effect of possible

faults. Different from PFTC, after fault occurrence, the first step of AFTC is to obtain fault information by FDD, then the second step is to tolerant faults by control redesign.

In the PFTC schemes, generally, fault tolerance is achieved without changing the controller. This implies that the controller is used to deal with all possible faults. Hence, the fault-tolerant ability of PFTC schemes is restrictive and can only adapt limited changes of the system induced by faults. With less flexibility, PFTC can only deal with a finite number of faults and the obtained solutions are suboptimal. Some PFTC approaches found in the literature are H_∞ robust control, adaptive compensation, quantitative feedback theory and variable structure control/sliding mode control. In [21], an overview of PFTC can be found.

Different from PFTC, AFTC includes FDD and control redesign. As said in [5], FDD includes the steps of fault detection, isolation, identification and estimation and can be implemented by means of a variety of methods, which are generally classified into model-based and data-based approaches. The model-based techniques use the mathematical models of the system as references to compare with the measured signals of the system. In the literature [72], the model-based methods include the four commonly used techniques: state estimation, parameter estimation, simultaneous/joint state & parameter estimation and parity space. The data-based techniques mainly include those methods using statistical methods, neural networks, fuzzy logic, etc.

The other step of AFTC is control redesign. In the AFTC schemes, after fault occurrence, the fault information can be obtained by FDD. Then, the obtained fault information is used to actively tolerate the effect of faults. Control redesign can be implemented by fault accommodation and control reconfiguration. Fault accommodation is limited to internal controller changes and adapts control parameters to the dynamics of the faulty system and the input and output of the plant remain the same as the nominal system, which means that the loop cannot be restructured. If fault accommodation cannot deal with faults, one has to reconfigure the control loop (i.e., control reconfiguration) to maintain stability and acceptable performance [5]. When using control reconfiguration, it means that the control loop has to be restructured to handle the faults and the controller parameters must be also adjusted to accommodate the changes in the faulty dynamics.

As reviewed in [72], the existing reconfigurable control design methods fall into pseudo inverse, gain scheduling/linear parameter varying, model following, adaptive control, multiple model, feedback linearization/dynamic inversion, MPC, generalized internal model control, neural networks, fuzzy logic, etc.

2.1.2 Set-based Fault Detection and Isolation

As aforementioned, FDI can be implemented by means of different methods. Under the framework of model-based FDI, for the systems with disturbances and noises, FDI

usually uses the methods such as Kalman filters and unknown input observers [14, 45, 63], where the priori knowledge of the distributions of disturbances and noises should be available. Differently, the proposed FDI methods in this dissertation are based on sets, which can provide FDI robustness by only requiring the bounds of disturbances and noises without need of their probabilistic distributions.

In the literature, there exist three commonly used set-based FD approaches, i.e., invariant set-based, interval observer-based, set membership estimation [2, 15, 17, 20, 40, 41, 44, 48, 54, 55, 57, 58, 60, 62]. The common feature of these FD approaches consists in testing consistency between the measured real-time signals and the reference signals estimated from the system models. For a faultless system, based on the nominal system model, one can construct a healthy invariant set to confine the residual in the nominal operation. Thus, as long as the system is healthy, the residual will always stay inside the healthy invariant set at steady state (this point will be further explained later). Thus, whenever it is detected that the residual goes out of its healthy invariant set, it implies that faults have occurred in the system. Please see [56, 57] for the details of this approach.

The interval observer-based method consists in designing an interval observer based on the nominal system model [18–20, 36, 39, 40, 47–49, 52]. Provided that an initial state set that contains the initial state of the system is given, the interval observer can estimate the upper and lower bounds of states and outputs in real time by using the measured inputs and outputs. FD based on interval observers is implemented by testing consistency between the measured outputs and their estimated bounds. If a violation is detected, it implies that the system has become faulty. Otherwise, it is still considered that the system is faultless.

Differently, the objective of set-membership estimation approaches is to robustly estimate the system states [2, 15, 29, 46, 54]. It is known that the real system is always affected by uncertainties such as disturbances and noises. It is impossible to obtain the accurate state values. The set-membership approaches estimate the sets of all possible states by two steps, i.e., prediction and correction steps. The prediction step uses the current system inputs and the estimated state set at the previous time instant to predict the state set at the current time instant. The correction step uses the current outputs to correct the predicted state set from the prediction step and obtains a more accurate state estimation set at the current time instant. If the state estimation set obtained after the prediction and correction steps is empty, it means that the system has become faulty. Otherwise, it is still considered that the system is healthy [7, 13].

Although all the aforementioned set-based approaches have been successfully used in FD, few works on the FI application of interval observers are proposed. Before, interval observer or set-membership estimation based fault diagnosis schemes generally rely on some other FI techniques [7, 47]. Thus, as one of the objectives of this research, this dissertation wants to implement interval observer-based FI and extend interval observers to the application of FTC.

2.1.3 Fault-tolerant Model Predictive Control

In [31], the inclusion of fault tolerance in MPC was proposed, where it is said that the basis for the proposal is that, since MPC relies on an explicit internal model, failures can be handled by updating the internal model and on-line optimizer can work out how to control the system in its new condition. In this dissertation, the proposed FTC schemes are implemented based on robust MPC strategies and set-based FDI methods. The objective of this dissertation is to exert the advantages of both MPC and set-based FDI. In this way, the proposed FTMPC schemes cannot only deal with multivariable constrained systems with uncertainties but also resist the effect of faults and generate optimal control actions under the framework of MPC.

In the literature, MPC is used for fault tolerance under either the PFTC or AFTC frameworks. In the case of PFTC, fault tolerance relies on robustness of MPC controllers [1]. It is known that MPC is an optimization-based control strategy. Thus, a degree of mismatch between the internal models of MPC controllers and those of the real system could be corrected in some sense. This endows MPC controllers with passive fault-tolerant capability. In [42], the passive and active FTMPC strategies are compared based on their applications in the Barcelona Sewer Network. Under the assumption that fault information can be ideally obtained and used for AFTC, the simulation results motivate the use of AFTC to implement control objectives. In [34], MPC with fault-tolerant function was applied to control the concentration and level of a solid crystal dissolution tank. In [59], MPC-based robust control is implemented for fault tolerance, where after faults, the system states are steered into a defined region to tolerate the effect of faults.

In the AFTC schemes, MPC controllers should be integrated with an FDI module, where the FDI module detects, diagnoses faults and provides fault information to the MPC controllers to implement fault-tolerant function. But, due to the effect of faults, it is difficult to cope with the issues related to feasibility guarantees, constraint satisfaction and state estimation in the FTMPC schemes. Generally, some existing AFTC schemes only investigate the effectiveness of MPC as the AFTC control strategy, where it is assumed that the FDI module is perfect and can obtain all needed fault information [16, 22, 42, 69]. In some other AFTC schemes, the FDI module is really designed and integrated into the FTMPC schemes, where the FDI mechanisms are designed by different FDI strategies. For example, in [63], an active FTMPC scheme using the Kalman filters is proposed, which focuses on the implementation of an active FTMPC scheme without considering the details such as feasibility guarantees. In [11], an active FTMPC scheme is implemented to show how MPC can be integrated into the AFTC schemes. In the literature, the existing works related to active FTMPC mainly focus on whether or not active FTMPC is implementable. As aforementioned, some related works assume that the FDI module is perfect and the fault information can be ideally obtained. But, in reality, these assumptions are impossible. This implies that some

proposed active FTMPC schemes are still far away from practical applications. More FTMPC works can be found in [9, 24, 33, 37, 54, 64].

This dissertation focuses on active FTMPC schemes with set-based FDI, which consider the aforementioned problems. Actually, there only exist few works related to active FTMPC implementation using set-based FDI. In [70, 71], FTMPC schemes integrating invariant set-based FDI are presented for actuator and sensor faults, respectively. The advantage of the schemes is its less computational complexity due to the use of tube-based MPC and invariant set-based FDI. However, due to passive implementation of FDI, it implies the loss of potential FDI performance in some sense if one wants to obtain FDI guarantees. In [51], an FTMPC scheme using the set-membership FDI approach is introduced, whose advantages consist in using an active FI method that can reduce FI conservatism. However, due to the requirements of computing separating inputs on-line, this approach has high complexity. Additionally, a method considering the design of separating inputs for active fault diagnosis is proposed in [50]. The feature of the method in [50] consists in that it computes separating inputs off-line and can reduce computational complexity with respect to the on-line computation of separating inputs, which perhaps can be integrated into an FTMPC framework. However, since the off-line computation of separating inputs is based on partitioning an output set that includes all possible outputs under all possible system modes (healthy or faulty), it is more conservative when comparing with the case of using the real-time measured outputs. Comparing with these approaches or schemes, this dissertation proposes active FTMPC schemes for actuator and sensor FTC with a balance between FDI conservatism, complexity and efficiency.

2.2 Research Tools

2.2.1 Polyhedral Sets

Polyhedra are a kind of fundamental geometric objects that have been widely investigated. The use of polyhedra is related to many fields such as fault diagnosis, state estimation, control and optimization. In what follows, one will recapitulate the background knowledge of polyhedra required in this research.

2.2.1.1 Polytopes

Polyhera are an useful convex geometrical representation of linear constraints in control and optimization. Polyhedra are formed by a group of half-spaces [4]. Because of the convexity, polyhedra own a good balance between complexity and flexibility. Polyhedra have dual mathematical representations, i.e., half-spaces (H-polyhedron) and vertices (V-polyhedron). The half-space representation is firstly introduced [4].

Definition 2.1. *An open half-space in $\mathbb{R}^n$ is the set $\{x \in \mathbb{R}^n : hx < v\}$ and a closed half-space in $\mathbb{R}^n$ is the set $\{x \in \mathbb{R}^n : hx \leq v\}$, where h is a vector with compatible dimensions and v is a scalar.*

Definition 2.2. *An H-polyhedron $P \subset \mathbb{R}^n$ is an intersection of a finite set of closed half-spaces with a form*

$$P = \{x \in \mathbb{R}^n : Fx \leq b, F \in \mathbb{R}^{m \times n}, b \in \mathbb{R}^m\}, \tag{2.1}$$

where $f_i x \leq b_i$ $(i = 1, 2, \ldots, m)$ is the i-th half-space, where f_i is the i-th row of F and b_i is the i-th component of b.

Remark 2.1. *In this dissertation, the inequalities should be understood elementwise. For example, the inequality (2.1) includes m elementwise inequalities.*

The V-polyhedron representation of polyhedra is based on the convex hull of a finite set of points and the cone of a finite set of vectors.

Definition 2.3. *A set S is said to be convex if for all $x_1 \in S$ and $x_2 \in S$, it satisfies*

$$\alpha x_1 + (1 - \alpha)x_2 \in S, \text{ for all } 0 \leq \alpha \leq 1.$$

Definition 2.4. *A C-set is a compact and convex set that contains the origin in its non-empty interior.*

Definition 2.5. *The image of a set S under a mapping M is defined as*

$$M(S) = \{y : y = M(x), x \in S\}.$$

Definition 2.6. *The convex hull of a set $V = \{v_1, v_2, \ldots, v_p\} \subset \mathbb{R}^n$ of points is defined as the set of all convex combinations of the points in V, i.e.,*

$$conv(V) = \{x : x = V\alpha, \sum_{i=1}^{p} \alpha_i = 1, \alpha \geq 0, \alpha \in \mathbb{R}^p\}, \tag{2.2}$$

where α_i is the i-th component of α and p denotes the number of points.

Definition 2.7. *The cone of a set $Y = \{y_1, y_2, \ldots, y_q\} \subset \mathbb{R}^n$ of vectors is defined as*

$$cone(Y) = \{y : y = Y\beta, \beta \geq 0, \beta \in \mathbb{R}^q\}, \tag{2.3}$$

where β_i is the i-th component of β and q denotes the number of vectors.

In order to give the definition of the V-polyhedron form, the Minkowski sum and Pontryagin difference of sets are given in Definitions 2.8 and 2.9, respectively.

Definition 2.8. *Given two sets $X_1 \subset \mathbb{R}^n$ and $X_2 \subset \mathbb{R}^n$, the Minkowski sum of the two sets is*

$$X_1 \oplus X_2 = \{x : x_1 + x_2, x_1 \in X_1, X_2 \in X_2\}.$$

Definition 2.9. *Given two sets $Y \subset \mathbb{R}^n$ and $Y_1 \subset \mathbb{R}^n$, the Pontryagin difference of the two sets is*

$$Y \ominus Y_1 = \{y_2 : y_1 + y_2 \in Y, \forall y_1 \in Y_1\}.$$

Based on the definitions of the convex set, the cone and the Minkowski sum in Definitions 2.3, 2.7 and 2.8, the V-polyhedron representation of polyhedra can be obtained.

Definition 2.10. *A V-polyhedron $P \subset \mathbb{R}^n$ is the Minkowski sum of the convex hull of a set $V = \{v_1, v_2, \ldots, v_p\} \subset \mathbb{R}^n$ of points and the cone of a finite set $Y = \{y_1, y_2, \ldots, y_q\} \subset \mathbb{R}^n$ of vectors, i.e.,*

$$P = conv(V) \oplus cone(Y). \tag{2.4}$$

The representation duality of polyhedra provides the flexibility for its wide applications. In some applications, the H-polyhedron representation is better to describe the problems, while in some others, the V-polyhedron representation may be more appropriate. This flexibility is based on the equivalence of the two representations.

Remark 2.2. *The H-polyhedron and V-Polyhedron representations of polyhedra are equivalent and these two representations can be converted into each other [73]. However, they are mathematically (but not algorithmically) equivalent.*

According to the aforementioned results of polyhedron, one can give the definition of polytopes as in Definition 2.11.

Definition 2.11. *A polytope is a polyhedron that is bounded.*

Remark 2.3. *An H-polytope is an H-polyhedron that is bounded and a V-polytope is a V-polyhedron that is bounded. Similarly, the H-polytope and V-Polytope are mathematically (but not algorithmically) equivalent.*

The operation of extracting the vertices of an H-polytope is called as vertex enumeration. The conversion between the H-polytope and V-polytope representations is implemented via vertex enumeration [8]. According to the results in [10], any convex body can be approximated arbitrarily well by a polytope. In this dissertation, polytopes are only used as the tool of set manipulations. Thus, only the knowledge of polytopes related to this research is presented here. For more details, the readers can be referred to the aforementioned relevant literature.

2.2.1.2 Zonotopes

Zonotopes are a special type of convex polytopes, which have the symmetric feature with respect to their centers. Zonotopes have two different but equivalent definitions. The first definition is based on the Minkowski sum of straight line segments and the second one is based on the image of hypercubes. In this research, the second definition is more interesting, which is formally given in Definition 2.12.

Definition 2.12. *An m-order zonotope Z is defined as $Z = g \oplus H\mathbb{B}^m$, where g and H are called the center and segment matrix (also generator matrix), respectively.*

The motivation to use zonotopes in this research consists in their geometric features, which can simplify the propagation of set-based dynamics.

Property 2.1. *Given two zonotopes $Z_1 = g_1 \oplus H_1\mathbb{B}^{m_1} \subset \mathbb{R}^n$ and $Z_2 = g_2 \oplus H_2\mathbb{B}^{m_2} \subset \mathbb{R}^n$, $Z_1 \oplus Z_2 = (g_1 + g_2) \oplus [H_1 \quad H_2]\mathbb{B}^{m_1+m_2}$.*

Property 2.2. *Given a zonotope $Z = g \oplus H\mathbb{B}^m \subset \mathbb{R}^n$ and a compatible matrix K, $KZ = Kg \oplus KH\mathbb{B}^m$.*

The smallest box containing a zonotope Z is called the interval hull of Z, who is defined in Definition 2.13.

Definition 2.13. *The interval hull $\square Z$ of a zonotope $Z = g \oplus H\mathbb{B}^m \subset \mathbb{R}^n$ is the smallest box containing Z, i.e.,*

$$\square Z = \{x : |x_i - g_i| \leq \| H_i \|_1\},$$

where H_i is the i-th row of H, x_i and g_i are the i-th components of x and g, respectively.

Definition 2.14. *The interval hull width of $Z = g \oplus H\mathbb{B}^m \subset \mathbb{R}^n$ is defined as a vector*

$$width(Z) = (2\|H_1\|_1, 2\|H_2\|_1, \ldots, 2\|H_n\|_1)^T,$$

where $2\|H_i\|_1$ denotes the width of the i-th interval component of $\square Z$.

The complexity of zonotopes is described by their order. The higher the order is, the more complex a zonotope is. In some applications, it is required to approximate high-order zonotopes with lower-order zonotopes. According to [15], a reduction method of zonotope complexity is presented in Property 2.3.

Property 2.3. *Given a zonotope $Z = g \oplus H\mathbb{B}^m \subset \mathbb{R}^n$ and an integer s (with $n < s < m$), denote by $\hat{H}$ the matrix resulting from the reordering of the columns of the matrix H in decreasing Euclidean norm. $Z \subseteq g \oplus [\hat{H}_T \quad Q]\mathbb{B}^s$ where $\hat{H}_T$ is obtained from the first $s - n$ columns of the matrix $\hat{H}$ and $Q \in \mathbb{R}^{n \times n}$ is a diagonal matrix whose elements satisfy $Q_{ii} = \sum_{j=s-n+1}^{m} | \hat{H}_{ij} |$, $i = 1, \ldots, n$.*

Definition 2.15. *A strip is defined as* $S = \{x : |cx - d| \leq \sigma\}$*, where* c *is a compatible vector, and* d *and* σ *are scalars.*

Moreover, in [2], a method to compute a zonotope that contains the intersection of a strip and a zonotope is given. Property 2.4 summarizes this method.

Property 2.4. *Given a zonotope* $Z = g \oplus H\mathbb{B}^m \subset \mathbb{R}^n$*, a strip* $S = \{x \in \mathbb{R}^n \mid |cx - d| \leq \sigma\}$ *and a vector* $\lambda \in \mathbb{R}^n$*, then* $Z \cap S \subseteq \hat{Z}(\lambda) = \hat{g}(\lambda) \oplus \hat{H}(\lambda)\mathbb{B}^{m+1}$ *holds, where* $\hat{g}(\lambda) = g + \lambda(d - cg)$ *and* $\hat{H}(\lambda) = [(I - \lambda c)H \quad \sigma\lambda]$.

Besides, a method proposed in [30] to compute a zonotope approximation of the intersection of a zonotope and a polytope is presented in Property 2.5.

Property 2.5. *Given a matrix* $\Lambda \in \mathbb{R}^{n\times m}$*, a zonotope* $Z = g \oplus H\mathbb{B}^r$*, and an* H*-polytope* $P = \{x \in \mathbb{R}^n : |Cx - d| \leq [\phi_1, \phi_2, ..., \phi_m]^T\}$*, with* $C \in \mathbb{R}^{m\times n}$*,* $d \in \mathbb{R}^m$*,* $\phi_i \in \mathbb{R}_+$ *(*$i = 1, 2, ..., m$*), define a vector* $\hat{g}(\Lambda) = g + \Lambda(d - Cg)$ *and a matrix* $\hat{H}(\Lambda) = [(I - \Lambda C)H \quad \Lambda\phi]$*, with a diagonal matrix* $\Lambda = diag(\phi_1, \phi_2, ..., \phi_m)$*. Then a family of zonotopes (parameterized by the matrix* Λ*) that contains the intersection of the zonotope* Z *and the polytope* P *is obtained such as* $Z \cap P \subseteq \hat{Z}(\Lambda) = \hat{g} \oplus \hat{H}\mathbb{B}^{r+m}$.

In this dissertation, the proposed set-based approaches propagate system uncertainties through the system model and the uncertainties are bounded by zonotopes. According to [2, 23], the properties related to zonotope inclusion are given in Properties 2.6 and 2.7.

Property 2.6. *Given a family of zonotopes denoted by* $Z = g \oplus \mathbf{H}\mathbb{B}^m$*, where* $g \in \mathbb{R}^n$ *is a vector and* $\mathbf{H} \in \mathbb{R}^{n\times m}$ *is an interval matrix, a zonotope inclusion* $\diamond(Z)$ *is defined by*

$$\diamond(Z) = g \oplus [mid(\mathbf{H}) \;\; H]\mathbb{B}^{m+n},$$

where the matrix H *is a diagonal matrix with*

$$H_{ii} = \sum_{j=1}^{m} \frac{diam(\mathbf{H})_{ij}}{2}, \; i = 1, 2, \cdots, n,$$

where $mid(\cdot)$ *and* $diam(\cdot)$ *compute the center and diameter of interval matrices.*

Property 2.7. *Given* $Z_{k+1} = \mathbf{A}Z_k \oplus \mathbf{B}u_k$*, where* $\mathbf{A}$ *and* $\mathbf{B}$ *are interval matrices and* u_k *is the input at time instant* k*, if* Z_k *is a zonotope with the center* g_k *and segment matrix* H_k*,* Z_{k+1} *can be bounded by a zonotope*

$$Z^e_{k+1} = g_{k+1} \oplus H_{k+1}\mathbb{B}^r,$$

with

$$\begin{aligned} g_{k+1} =& mid(\mathbf{A})g_k + mid(\mathbf{B}))u_k, \\ H_{k+1} =& [J_1 \quad J_2 \quad J_3], \\ J_1 =& seg(\diamond(\mathbf{A}H_k)), \\ J_2 =& \frac{diam(\mathbf{A})}{2} g_k, \\ J_3 =& \frac{diam(\mathbf{B})}{2} u_k, \end{aligned}$$

where $seg(\cdot)$ computes the segment matrix of a zonotope.

Zonotopes are used as the containment sets in this research. In propagation of the set-based dynamics, the advantage of zonotopes consists in their balance among compactness, complexity and precision (see [47, 48] for the applications of zonotopes in interval methods). In reality, the system constraints and uncertainties are often described by convex sets. Since it is possible to approximate convex sets by zonotopes, with a degree of approximations, zonotopes can always be used. However, zonotopes are just one choice and their applications should consider the particular situations.

2.2.2 Invariant Sets

This section introduces the basic set invariance notions related to the linear discrete time-variant dynamics. These notions are the important basis of the proposed approaches in this research.

2.2.2.1 Robust Positively Invariant Set

One firstly considers the notions of PI and RPI sets corresponding to the dynamics free from or affected by process disturbances, respectively.

Definition 2.16. *A set X is a PI set of the dynamics $x_{k+1} = f(x_k)$ if for any $x_k \in X$, one has $x_{k+1} \in X$ for all $k \geq 0$.*

Definition 2.17. *A set X is an RPI set of the dynamics $x_{k+1} = f(x_k, \omega_k)$ if for $x_k \in X$ and $\omega_k \in W$, one always has $x_{k+1} \in X$.*

Definition 2.18. *The mRPI set of the dynamics is defined as an RPI set contained in any closed RPI set and the mRPI set is unique and compact.*

Definition 2.19. *A Schur matrix is a square matrix composed of real entries and with all its eigenvalues inside the unit circle.*

In this dissertation, one focuses on the linear discrete time-invariant dynamics with process perturbation, which are modelled as

$$x_{k+1} = Ax_k + E\omega_k, \tag{2.6}$$

where A and E are constant matrices with suitable dimensions, x_k is the state of the dynamics at time instant k, and ω_k is the bounded process disturbance with $\omega_k \in W = \{\omega : |\omega - \omega^c| \leq \bar{\omega}\}$, where the vectors ω^c and $\bar{\omega}$ are constant.

According to the results in [25, 44], one gives the following method to construct the RPI sets of the dynamics (2.6).

Theorem 2.1. *Considering the dynamics (2.6) and letting $A = V\Lambda V^{-1}$ be the Jordan decomposition, the set*

$$\Phi(\theta) = \{x : \left|V^{-1}x\right| \leq (I - |\Lambda|)^{-1} \left|V^{-1}E\right| \bar{\omega} + \theta\} \oplus \xi^{\circ}$$

is RPI and attractive for the trajectories of the dynamics (2.6), with θ being any (arbitrarily small) vector with positive components, where $\xi^{\circ} = (I - A)^{-1}E\omega^c$.

1. *For any θ, the set $\Phi(\theta)$ is (positively) invariant, that is, if $x_0 \in \Phi(\theta)$, then $x_k \in \Phi(\theta)$ for all $k \geq 0$.*
2. *Given $\theta > 0$ and x_0, there exists $k^* \geq 0$ such that $x_k \in \Phi(\theta)$ for all $k \geq k^*$.*

Proposition 2.1. *Considering the dynamics (2.6) and denoting X_0 as an initial set of the dynamics, the set sequence*

$$X_{j+1} = AX_j \oplus EW, \quad j \in \mathbb{N}$$

converges to the mRPI set of the dynamics (2.6), where if X_0 is an RPI set, each iteration of the set sequence is an RPI approximation of the mRPI set.

Remark 2.4. *Using Proposition 2.1, one can obtain an RPI approximation of the mRPI set of the dynamics (2.6) with any expected precision.*

Definition 2.20. *Given a scalar $\epsilon > 0$ and a set $\Omega \subset \mathbb{R}^n$, the set $\Phi \subset \mathbb{R}^n$ is an outer ϵ-approximation of Ω if $\Omega \subseteq \Phi \subseteq \Omega \oplus \mathbb{B}_s^n(\epsilon)$ and it is an inner ϵ-approximation of Ω if $\Phi \subseteq \Omega \subseteq \Phi \oplus \mathbb{B}_s^n(\epsilon)$, where $\mathbb{B}_s^n(\epsilon) = \{x \in \mathbb{R}^n : \| x \|_s \leq \epsilon\}$.*

By means of the set invariance notions, the RPI sets of the linear discrete time-variant dynamics can be constructed.

2.2.2.2 Robust Controlled Invariant Sets

When the system is subject to the external inputs and system constraints, one should consider the CI sets. For all $k \geq 0$, the system state and input constraints are defined as

$$x_k \in X, \tag{2.7a}$$
$$u_k \in U. \tag{2.7b}$$

Definition 2.21. *A set $\mathcal{C} \subseteq X$ is a CI set of the dynamics $x_{k+1} = f(x_k, u_k)$ if for any $x_k \in \mathcal{C}$, there always exists $u_k \in U$ such that $x_{k+1} \in \mathcal{C}$ holds for all $k \geq 0$.*

Definition 2.22. *A set $\mathcal{C}_\mathcal{M} \subseteq X$ is said to be the MCI set of the dynamics $x_{k+1} = f(x_k, u_k)$, if it is CI and contains all CI sets inside X.*

Moreover, for the dynamics affected by process disturbances $\omega_k \in W$, one should consider the RCI sets.

Definition 2.23. *A set $\mathcal{O} \subseteq X$ is an RCI set of the dynamics $x_{k+1} = f(x_k, u_k, \omega_k)$ if for any $x_k \in \mathcal{O}$, there always exists $u_k \in U$ for any $\omega_k \in W$ such that $x_{k+1} \in \mathcal{O}$ holds for all $k \geq 0$.*

Definition 2.24. *A set $\mathcal{O}_\mathcal{M} \subseteq X$ is said to be the MRCI set of the dynamics $x_{k+1} = f(x_k, u_k, \omega_k)$, if it is RCI and contains all RCI sets inside X.*

In this dissertation, one only focuses on the linear discrete time-invariant dynamics subject to process disturbances and state and input constraints, and the construction of the RCI and MRCI sets of the linear discrete time-invariant dynamics is based on the back-forward iteration algorithm, which is omitted here. However, the interested reader can find all relevant knowledge in [8].

2.2.3 Robust Model Predictive Control

2.2.3.1 Model Predictive Control

MPC is a successful advanced control strategy in process industry and is implemented by on-line optimization. For the discrete-time dynamics

$$x_{k+1} = f(x_k, u_k) \tag{2.8}$$

that describes the evolution of states x_k under the manipulated inputs u_k starting from an initial state, one can consider an objective function

$$\min_{\mathbf{u}} \sum_{k=0}^{N-1} q(x_k, u_k) + p(x_N), \tag{2.9}$$

where $\mathbf{u} = [u_0, u_1, \ldots, u_{N-1}]$ is the control sequence by optimizing (2.9) over the prediction horizon N, and $q(x_k, u_k)$ and $p(x_N)$ are the stage and terminal cost functions.

The basic principle of MPC is that it uses the system model (2.8) to obtain the state predictions over the horizon N and then solves the objective function (2.9) to obtain the optimal control sequence over the prediction horizon. Note that solving the objective function at each time instant is based on the real-time measurements/estimations of states. Only the first element of the obtained control sequence is injected into the controlled system and the whole on-line optimization procedure is repeated at each time instant [8, 32].

The success of MPC stems from the fact that it can effectively deal with the system with interactions, constraints or multivariables, which would be hard for any other control strategy to accomplish. The limitation of MPC is that the on-line optimization algorithm at each time instant requires substantial time and computational resources. However, fast computational platforms together with advances in the field have significantly increased the MPC applicability to fast-sampled applications [8, 32].

2.2.3.2 Tube-based Model Predictive Control

The previous subsection has introduced the basic principle of MPC. The conventional MPC technique is not robust to the effect of uncertainties. In order to deal with system uncertainties, it is necessary to consider robust MPC techniques. In the literature, there exist two important types of robust MPC techniques, i.e., the tube-based and min-max techniques. This part briefly introduces tube-based robust MPC.

For the linear time-invariant systems with additive process disturbances, the advantage of tube-based MPC is that it has relatively low computational complexity. The tube-based MPC technique used in this dissertation is referred to [35]. The linear discrete time-invariant plant is modelled as

$$x_{k+1} = Ax_k + Bu_k + \omega_k, \tag{2.10a}$$
$$y_k = Cx_k + \eta_k, \tag{2.10b}$$

where the matrices B and C are constant, and y_k and η_k denote the output vector and measurement noise. The state and input hard constraints of the system are denoted as (2.7) and it is assumed that η_k is bounded by

$$\eta_k \in V. \tag{2.11a}$$

Because of the effect of the process disturbance and measurement noise, it is impossible to obtain the accurate values of system states. Nevertheless, in order to generate control inputs, one has to estimate the system states. For tube-based MPC, a Luen-

berger observer based on (2.10) is designed as

$$\hat{x}_{k+1} = (A - LC)\hat{x}_k + Bu_k + Ly_k, \tag{2.12a}$$
$$\hat{y}_k = C\hat{x}_k, \tag{2.12b}$$

where $\hat{x}_k$ and $\hat{y}_k$ are the estimated states and outputs and L is the observer gain that can stabilize the observer.

The nominal system corresponding to the actual system (2.10) is obtained by neglecting the uncertainties ω_k and η_k from (2.10), i.e.,

$$\bar{x}_{k+1} = A\bar{x}_k + B\bar{u}_k, \tag{2.13a}$$
$$\bar{y}_k = C\bar{x}_k, \tag{2.13b}$$

where $\bar{x}_k$, $\bar{u}_k$ and $\bar{y}_k$ are the nominal state, input and output vectors at time instant k. Thus, the open-loop optimization problem of the tube-based MPC controller, based on the nominal system (2.13), has the following form

$$\begin{aligned} J_k = \min_{\bar{\mathbf{u}}} \sum_{j=0}^{N-1} & \|(\bar{x}_{k+j|k} - \bar{x}^*)\|_{\bar{Q}}^2 + \|(\bar{u}_{k+j|k} - \bar{u}^*)\|_{\bar{R}}^2 + \|(\bar{x}_{k+N|k} - \bar{x}^*)\|_{\bar{P}}^2 \\ \text{subject to} \quad & \bar{x}_{k+j|k} \in \bar{X}, \\ & \bar{u}_{k+j|k} \in \bar{U}, \\ & \bar{x}_{k+N|k} \in \bar{X}_T, \\ & \bar{x}_{k|k} = \bar{x}_k, \end{aligned} \tag{2.14}$$

where $\bar{\mathbf{u}} = [\bar{u}_{k|k}, \bar{u}_{k+1|k}, \ldots, \bar{u}_{k+N-1|k}]$ is the generated control sequence, $\bar{x}_{k+j|k}$ is the j-th state prediction of the nominal system at time instant k, $\bar{x}^*$ and $\bar{u}^*$ are a state-input setpoint pair, $\bar{Q}$, $\bar{R}$ and $\bar{P}$ are positive-definite matrices and $\bar{X}$, $\bar{U}$ and $\bar{X}_T$ are the state, input and terminal state constraints of the nominal system (2.13). Note that, in (2.14), the construction of $\bar{X}$, $\bar{U}$ and $\bar{X}_T$ will be detailed in Chapter 6.

Based on the observer (2.12) and open-loop optimization problem (2.14), the control law of the tube-based MPC controller has the following form

$$u_k = \bar{u}_k + K(\hat{x}_k - \bar{x}_k), \tag{2.15}$$

where K is the feedback gain designed for this tube-based MPC controller.

Remark 2.5. *For brevity, this part only introduces the principle of tube-based MPC and it is assumed that the tube-based MPC controller shown in this section can stabilizable the system. The details on the tube-based MPC technique used in this dissertation can be found in [35].*

2.2.3.3 Min-max Model Predictive Control

The other robust MPC technique used in this research is the min-max robust MPC technique. This is the application of the min-max approach in the MPC framework

and extends the use of MPC to robustly resist the effect of uncertainties. A min-max strategy in MPC means that the worst-case performance with respect to uncertainties is optimized. The limitation of min-max MPC consists in its computational complexity in order to obtain robustness against uncertainties, while its most important advantage over tube-based MPC in this research is that it can directly manipulate the input constraints of the plant[1]. This is very helpful in the implementation of proposed FTMPC schemes. The details will be presented in the following chapters. The readers can see [28] for more details of the min-max MPC technique. For the system (2.10), the robust MPC controller is designed as

$$
\begin{aligned}
J_k = \min_{\mathbf{u}} \max_{\mathbf{w}} & \sum_{j=0}^{N-1} \|(x_{k+j|k} - x^*)\|_Q^2 + \|(u_{k+j|k} - u^*)\|_R^2 + \|(x_{k+N|k} - x^*)\|_P^2 \\
\text{subject to} \quad & \left.\begin{aligned} x_{k+j|k} &\in X, \\ u_{k+j|k} &\in U, \\ x_{k+N|k} &\in X_T, \\ x_{k|k} &= \hat{x}_k, \end{aligned}\right\} \forall \omega_{k+j|k} \in W,
\end{aligned} \tag{2.16}
$$

where x^* and u^* are a state-input setpoint pair, X_T is the terminal state constraint set (defined as the MRCI set corresponding to the state and input constraint sets X and U), $\mathbf{u} = [u_{k|k}, u_{k+1|k}, \ldots, u_{k+N-1|k}]$, Q, R and P are positive-definite weighting matrices, $\mathbf{w} = [\omega_{k|k}, \omega_{k+1|k}, \ldots, \omega_{k+N-1|k}]$ and the internal model of the min-max MPC controller is given as

$$
x_{k+j+1|k} = Ax_{k+j|k} + Bu_{k+j|k} + \omega_{k+j|k}. \tag{2.17}
$$

Over the prediction horizon N, the state prediction $x_{k+j|k}$ and manipulated input $u_{k+j|k}$ at time instant k are subject to the internal model (2.17). Eventually, the optimization problem (2.16) is solved and the control sequence $\mathbf{u}$ is obtained. According to the MPC principle introduced in this section, at time instant k, only the first element of $\mathbf{u}$ is used as the current control input vector and is injected into the system. Afterwards, the optimization problem (2.16) is repeated at each time instant to generate control inputs in real time.

2.3 Summary

This chapter introduces some fundamental notions and summarizes the state of the art of the research area. In the literature, some existing works related to this research

[1]The tube-based MPC controller indirectly guarantees the input constraint satisfaction as in (2.7) by directly manipulating the input of the nominal system (2.13) such that $\hat{u}_k \in \bar{U}$. But during the transition induced by faults, because the system model is changed, the input constraint satisfaction cannot be guaranteed again. Comparatively, because the min-max MPC controller directly manipulates the plant inputs, the input constraint satisfaction can always be guaranteed as long as the min-max MPC controller is always feasible.

are also reviewed in this chapter. Besides, This chapter also introduces research tools involved in this research, which are polyhedra, invariant sets and robust MPC. Considering that the objective of this chapter is to introduce the background knowledge related to this dissertation, not all details of these knowledge are presented and one mainly gives the general picture. Thus, for more details, the readers are suggested to read the mentioned literature of set theory and robust MPC.

Part II

Fault Detection and Isolation

Chapter 3

Invariant Sets and Interval Observers

This chapter introduces interval observers and invariant sets and their applications in fault diagnosis. Most importantly, the objective of this chapter is to investigate the relationship of interval observers and invariant sets and to discuss their advantages and disadvantages, respectively.

3.1 Problem Formulation

In order to explain the FD principles of interval observers and invariant sets, one considers a fundamental system framework, which is shown in Figure 3.1.

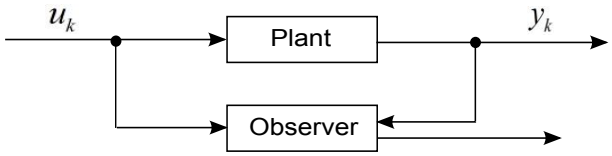


Figure 3.1: System framework

For brevity, in this chapter, the linear discrete time-invariant plant is redefined as

$$x_{k+1} = Ax_k + Bu_k + \omega_k, \tag{3.1a}$$

$$y_k = Cx_k + \eta_k, \tag{3.1b}$$

where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times p}$ and $C \in \mathbb{R}^{q\times n}$ are constant parametric matrices, $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^p$ and $y_k \in \mathbb{R}^q$ are state, input and output vectors, respectively, $\omega_k \in W$ and $\eta_k \in V$ are the bounded process disturbance and measurement noise, respectively, and k denotes the k-th discrete time instant. The bounding sets W and V are defined as

$$W = \{\omega \in \mathbb{R}^n : \ |\omega - \omega^c| \leq \bar{\omega}, \omega^c \in \mathbb{R}^n, \bar{\omega} \in \mathbb{R}^n\}, \tag{3.2a}$$

$$V = \{\eta \in \mathbb{R}^q : \ |\eta - \eta^c| \leq \bar{\eta}, \eta^c \in \mathbb{R}^q, \bar{\eta} \in \mathbb{R}^q\}, \tag{3.2b}$$

where ω^c, η^c, $\bar{\omega}$ and $\bar{\eta}$ are constant vectors. It can be observed that the sets W and V can be rewritten as zonotopes

$$W = \omega^c \oplus H_{\bar{\omega}}\mathbb{B}^n, \tag{3.3a}$$
$$V = \eta^c \oplus H_{\bar{\eta}}\mathbb{B}^q, \tag{3.3b}$$

where $H_{\bar{\omega}} \in \mathbb{R}^{n\times n}$ and $H_{\bar{\eta}} \in \mathbb{R}^{q\times q}$ are two diagonal matrices with their diagonal entries composed of $\bar{\omega}$ and $\bar{\eta}$, respectively.

Assumption 3.1. *The system described in Figure 3.1 is stable and the pair (A,C) is detectable.*

3.2 Invariant Sets in Fault Detection

For the system shown in Figure 3.1, if the invariant set-based approach is used to implement fault diagnosis, according to [41, 44, 55, 57, 58], a Luenberger observer based on the model (3.1) should be designed as

$$\hat{x}_{k+1} = A\hat{x}_k + Bu_k + L(y_k - C\hat{x}_k), \tag{3.4a}$$
$$\hat{y}_k = C\hat{x}_k, \tag{3.4b}$$

where $\hat{x}_k$ and $\hat{y}_k$ are the estimated state and output at time instant k, and L is the observer gain matrix designed to assure the contractiveness of the observer. Note that the contractiveness of the observer (3.4) is always possible under Assumption 3.1.

Furthermore, according to the measured output vector y_k and the estimated output vector $\hat{y}_k$, one can define a residual for the invariant set-based FD method as

$$\begin{aligned} r_k^{is} =& y_k - \hat{y}_k \\ =& C\tilde{x}_k + \eta_k, \end{aligned} \tag{3.5}$$

where r_k^{is} denotes the residual at time instant k, the superscript is denotes *invariant sets*, and the state estimation error $\tilde{x}_k$ of the observer is defined as

$$\tilde{x}_k = x_k - \hat{x}_k.$$

Furthermore, by using (3.1) and (3.4), the dynamics of $\tilde{x}_k$ can be derived as

$$\tilde{x}_{k+1} = (A - LC)\tilde{x}_k - L\eta_k + \omega_k. \tag{3.6}$$

It is known that ω_k and η_k are bounded. Thus, one can construct an RPI set to confine $\tilde{x}_k$ as in (3.6) [25, 44]. The resultant RPI set of $\tilde{x}_k$ is denoted as $\Phi^{\tilde{x}}$ and the corresponding set to confine the residual is computed as

$$R^{is} = C\Phi^{\tilde{x}} \oplus V. \tag{3.7}$$

According to the definition of the RPI sets, once $\tilde{x}_k$ enters into its RPI set $\Phi^{\tilde{x}}$, then it will always remain inside the RPI set and the same result holds for the residual r_k^{is}. Thus, as long as $\tilde{x}_k \in \Phi^{\tilde{x}}$ holds, one will always have

$$r_k^{is} \in R^{is}. \tag{3.8}$$

The invariant set-based FD method consists in testing whether or not the residual r_k^{is} strictly belongs to its healthy set R^{is} in real time. If, at one time, the residual exits its healthy set, it is indicated that the system has become faulty[1]. Otherwise, it is considered that the system is still healthy.

Remark 3.1. *If needed, one can also add ω^c and η^c into (3.4). However, in the case that ω^c and η^c are not zero, it means that one only adds an offset to the corresponding invariant set, which does not affect general conclusions presented in this chapter.*

3.3 Interval Observers in Fault Detection

Instead of invariant sets, if interval observers are used for fault diagnosis, the plant should be monitored by an interval observer, which takes the worst case of uncertainties into account. The set-based form of the interval observer, based on the plant model (3.1), is designed as

$$\hat{X}_{k+1} = (A - LC)\hat{X}_k \oplus \{Bu_k\} \oplus \{Ly_k\} \oplus (-L)V \oplus W, \tag{3.9a}$$
$$\hat{Y}_k = C\hat{X}_k \oplus V, \tag{3.9b}$$

where $\hat{X}_k$ and $\hat{Y}_k$ are the estimated state and output sets at time instant k, respectively, and L is the observer gain matrix that is chosen to guarantee the set-mapping contractiveness of the interval observer and the avoidance of the wrapping effect [39].

Note that the interval observer (3.9) is designed based on a Luenberger observer

$$\hat{x}_{k+1} = A\hat{x}_k + Bu_k + L(y_k - C\hat{x}_k) + \breve{\omega}_k, \tag{3.10a}$$
$$\hat{y}_k = C\hat{x}_k + \breve{\eta}_k, \tag{3.10b}$$

where the signals $\breve{\omega}_k$ and $\breve{\eta}_k$ are artificial and bounded, i.e., $\breve{\omega}_k \in W$ and $\breve{\eta}_k \in V$, which are used to simulating the effect of ω_k and η_k on the plant (3.1).

[1] In this dissertation, the terms such as *faults*, *become faulty*, *fault occurrence*, *fault detection and isolation* and *fault-tolerant control* are generally related to the mode switching among different faulty modes, fault detection from healthy to faulty and system recovery from faulty to healthy as long as the proposed approaches can deal with these situations.

Remark 3.2. *Theoretically, the observer gain matrices of* (3.9) *and* (3.4) *can be designed separately. But, for the sake of comparing the two FD approaches, one uses the same observer gain L for both* (3.9) *and* (3.4)*. However, one should notice that the observer gain can affect the effectiveness of the fault diagnosis approaches. Please see [40] for more information on this point.*

Using zonotope operations in Section 2.2.1, (3.9) can be transformed into the center-segment matrix form. Thus, the centers $\hat{x}^c_{k+1}$ and $\hat{y}^c_k$ and segment matrices $\hat{H}^x_{k+1}$ and $\hat{H}^y_k$ of $\hat{X}_{k+1}$ and $\hat{Y}_k$ can be computed as

$$\hat{x}^c_{k+1} = (A - LC)\hat{x}^c_k + Bu_k + Ly_k - L\eta^c + w^c, \tag{3.11a}$$

$$\hat{H}^x_{k+1} = [(A - LC)\hat{H}^x_k \quad -LH_{\bar{\eta}} \quad H_{\bar{\omega}}], \tag{3.11b}$$

$$\hat{y}^c_k = C\hat{x}^c_k + \eta^c, \tag{3.11c}$$

$$\hat{H}^y_k = [C\hat{H}^x_k \quad H_{\bar{\eta}}]. \tag{3.11d}$$

Assumption 3.2. *The initial state of the plant is denoted as x_0 and x_0 belongs to the initial zonotope $\hat{X}_0$ of the interval observer.*

Remark 3.3. *The initial set $\hat{X}_0$ can be arbitrarily assigned if necessary, which means that it is always possible to find a set to bound x_0. Additionally, this also implies the designing flexibility of the interval observer-based approach at the initial phase.*

In order to implement the interval observer-based FD, a residual should be defined. However, the residual definition here is different from the conventional one, which is in terms of sets, i.e.,

$$\begin{aligned} R^{io}_k =& \{y_k\} \oplus (-\hat{Y}_k) \\ =& \{Cx_k + \eta_k\} \oplus \{(-C\hat{X}_k) \oplus (-V)\} \\ =& C\{\{x_k\} \oplus (-\hat{X}_k)\} \oplus \{\eta_k\} \oplus (-V), \end{aligned} \tag{3.12}$$

where R^{io}_k denotes the residual zonotope at time instant k and the superscript *io* represents *interval observers*.

In (3.11), it can be observed that, as k increases, the order of segment matrices of residual zonotopes grows dramatically. In order to propagate the dynamics of the interval observer, it is necessary to control the order of zonotopes. In Property 2.3, a method is proposed to reduce the complexity of zonotopes by using low-order zonotopes to over-approximate high-order zonotopes.

Under Assumption 3.2, when the interval observer (3.9) is used to monitor the dynamic behaviors of the system, as long as the system is healthy, the residual zonotopes should always contain the origin. Thus, the interval observer-based FD method consists in checking whether or not

$$\mathbf{0} \in R^{io}_k \tag{3.13}$$

is violated in real time, where $\mathbf{0}$ is the origin. If (3.13) is violated, it means that the system has become faulty. Otherwise, it is considered that the system is still in the healthy operation. More details on the FD application of interval observers can be referred to [18–20, 36, 39, 40, 47–49, 52].

Note that, sometimes, instead of checking (3.13), another relatively rough but simple consistency-testing method is to test whether or not

$$\mathbf{0} \in \square R_k^{io}$$

holds for FD, where $\square R_k^{io}$ denotes the interval hull of the residual zonotope R_k^{io}.

Remark 3.4. *Since the computation of state and output intervals is based on the interval hull of zonotopes, for brevity, all discussions are directly based on zonotopes in the sequel.*

3.4 Relationship of Invariant Sets and Interval Observers

In this section, the relationship of interval observers and invariant sets is briefly investigated, which is based on the results in [68].

3.4.1 Bounds of Interval Observers

In order to analyze residual zonotopes defined in (3.12) for the interval observer-based approach, a zonotope

$$\begin{aligned}\tilde{X}_k =& \{x_k\} \oplus (-\hat{X}_k) \\ =& (x_k - \hat{x}_k^c) \oplus \hat{H}_k^x \mathbb{B}^{s_k}\end{aligned} \tag{3.14}$$

is defined, where s_k denotes the order of $\tilde{X}_k$ and $\hat{X}_k$ is denoted as

$$\hat{X}_k = \hat{x}_k^c \oplus \hat{H}_k^x \mathbb{B}^{s_k}.$$

Using the notations $\tilde{x}_k^c$ and $\tilde{H}_k$ to denote $x_k - \hat{x}_k^c$ and $\hat{H}_k^x$, respectively, $\tilde{X}_k$ is rewritten as

$$\tilde{X}_k = \tilde{x}_k^c \oplus \tilde{H}_k \mathbb{B}^{s_k}.$$

Furthermore, taking into account (3.1a), (3.11a) and (3.11b), the center and segment matrix of $\tilde{X}_{k+1}$ can be derived as

$$\tilde{x}_{k+1}^c = (A - LC)\tilde{x}_k^c - L(\eta_k - \eta^c) + (\omega_k - \omega^c), \tag{3.15a}$$

$$\tilde{H}_{k+1} = \hat{H}_{k+1}^x = [(A - LC)\hat{H}_k^x \quad -LH_{\bar{\eta}} \quad H_{\bar{\omega}}]. \tag{3.15b}$$

According to zonotope operations, an equivalent zonotope-based form of (3.15) can be deduced as

$$\tilde{X}_{k+1} = (A - LC)\tilde{X}_k \oplus (-L)[(\eta_k - \eta^c) \oplus H_{\bar{\eta}}\mathbb{B}^q] \oplus [(\omega_k - \omega^c) \oplus H_{\bar{\omega}}\mathbb{B}^n]. \tag{3.16}$$

According to the expression (3.14), the left side of (3.16) can be rewritten as

$$\begin{aligned}\tilde{X}_{k+1} =& \tilde{x}^c_{k+1} \oplus \tilde{H}_{k+1}\mathbb{B}^{s_{k+1}} \\ =& (x_{k+1} - \hat{x}^c_{k+1}) \oplus \hat{H}^x_{k+1}\mathbb{B}^{s_{k+1}} \\ =& \{x_{k+1}\} \oplus [(-\hat{x}^c_{k+1}) \oplus \hat{H}^x_{k+1}\mathbb{B}^{s_{k+1}}],\end{aligned} \tag{3.17}$$

while the right side of (3.16) can be rewritten as

$$\begin{aligned}\tilde{X}_{k+1} =& (A - LC)[(x_k - \hat{x}^c_k) \oplus \hat{H}^x_k\mathbb{B}^{s_k}] \oplus (-L)[(\eta_k - \eta^c) \oplus H_{\bar{\eta}}\mathbb{B}^q] \\ & \oplus [(\omega_k - \omega^c) \oplus H_{\bar{\omega}}\mathbb{B}^n] \\ =& \{(A - LC)x_k\} \oplus (A - LC)[(-\hat{x}^c_k) \oplus \hat{H}^x_k\mathbb{B}^{s_k}] \oplus \{(-L)\eta_k\} \\ & \oplus (-L)[(-\eta^c) \oplus H_{\bar{\eta}}\mathbb{B}^q] \oplus \{\omega_k\} \oplus [(-\omega^c) \oplus H_{\bar{\omega}}\mathbb{B}^n].\end{aligned} \tag{3.18}$$

When (3.9) estimates state and output zonotopes, one only uses the bounds of the disturbance and noise, which corresponds to the worst case of the considered uncertainties in the plant. It can be observed that the expressions (3.17) and (3.18) correspond to $x_{k+1} - \hat{x}_{k+1}$ and $(A - LC)(x_k - \hat{x}_k) - L\eta_k + \omega_k + L\breve{\eta}_k - \breve{\omega}_k$, respectively. Using $\breve{x}_k$ to characterize $x_k - \hat{x}_k$, one obtains the corresponding equivalent dynamics of (3.16)[1]

$$\breve{x}_{k+1} = (A - LC)\breve{x}_k - L\eta_k + \omega_k + L\breve{\eta}_k - \breve{\omega}_k. \tag{3.19}$$

If considering W and V into (3.19), a set-based form of (3.19) can be obtained as

$$\breve{X}_{k+1} = (A - LC)\breve{X}_k \oplus (-L)V \oplus W \oplus LV \oplus (-W). \tag{3.20}$$

By using zonotope operations, the center $\breve{x}^c_{k+1}$ and segment matrix $\breve{H}_{k+1}$ of $\breve{X}_{k+1}$ described by (3.20) can be derived as

$$\breve{x}^c_{k+1} = (A - LC)\breve{x}^c_k, \tag{3.21a}$$

$$\breve{H}_{k+1} = [(A - LC)\breve{H}_k \quad -LH_{\bar{\eta}} \quad H_{\bar{\omega}} \quad LH_{\bar{\eta}} \quad -H_{\bar{\omega}}]. \tag{3.21b}$$

By comparing (3.16) and (3.20), it is shown that zonotopes estimated by (3.20) bound those estimated by (3.16) at each time instant, as long as the initial condition $\tilde{X}_0 \subseteq \breve{X}_0$ holds. Finally, according to (3.12) and (3.20), zonotopes bounding residual zonotopes can be derived as

$$\breve{R}^{io}_k = C\breve{X}_k \oplus V \oplus (-V). \tag{3.22}$$

[1] $x_k - \hat{x}_k$ is different from $\tilde{x}_k = x_k - \hat{x}_k$ in (3.5). The former corresponds to interval observers while the latter corresponds to invariant sets. Thus, the notations $\breve{x}_k$ and $\tilde{x}_k$ are used to distinguish them.

3.4.2 Relationship in Terms of Intermediate Sets

An RPI set of the dynamics (3.6) can be constructed by Theorem 2.1, which is denoted as $\Phi_0^{\tilde{x}}$ with the center ξ_0^c (since W and V are zonotopes, the construction of $\Phi_0^{\tilde{x}}$ implies that it can also be denoted as a zonotope). According to Proposition 2.1 and using the RPI set $\Phi_0^{\tilde{x}}$ as an initial set, another squeezed RPI set with an arbitrarily expected precision to the mRPI set of (3.6) can be obtained by iterating

$$\Phi_{j+1}^{\tilde{x}} = (A - LC)\Phi_j^{\tilde{x}} \oplus (-L)V \oplus W,\ j \in \mathbb{N}, \tag{3.23}$$

where j represents the j-th element of this set sequence. Moreover, (3.23) can be unfolded into the same form as that of (3.15), with the center ξ_{j+1}^c and segment matrix $H_{j+1}^{\tilde{x}}$ being

$$\xi_{j+1}^c = (A - LC)\xi_j^c - L\eta^c + \omega^c, \tag{3.24a}$$

$$H_{j+1}^{\tilde{x}} = [(A - LC)H_j^{\tilde{x}} \quad -LH_{\bar{\eta}} \quad H_{\bar{\omega}}]. \tag{3.24b}$$

In Proposition 2.1, as j tends to infinity, the set sequence (3.23) converges to the mRPI set of (3.6), which is denoted as $\Phi_\infty^{\tilde{x}}$ with the center ξ_∞^c. Furthermore, comparing (3.15), (3.21) and (3.24) with each other, as k and j tend to infinity, one has

$$\tilde{x}_\infty^c = [I - (A - LC)]^{-1}[(\omega_\infty - L\eta_\infty) - (\omega^c - L\eta^c)], \tag{3.25a}$$

$$\breve{x}_\infty^c = \mathbf{0}, \tag{3.25b}$$

$$\xi_\infty^c = [I - (A - LC)]^{-1}(\omega^c - L\eta^c), \tag{3.25c}$$

$$\| \tilde{H}_{\infty_i} \|_1 = \| H_{\infty_i}^{\tilde{x}} \|_1 \leq \| \breve{H}_{\infty_i} \|_1, \tag{3.25d}$$

where i represents the i-th row of a matrix and $\omega_\infty \in W$ and $\eta_\infty \in V$ are unknown, bounded and random variables. Thus, the centers of $\tilde{X}_\infty$ and $\Phi_\infty^{\tilde{x}}$ have the relationship $\tilde{x}_\infty^c + \xi_\infty^c = [I - (A - LC)]^{-1}(\omega_\infty - L\eta_\infty)$, where because ω_∞ and η_∞ are bounded, $\tilde{x}_\infty^c + \xi_\infty^c$ are also bounded, whose bounds can be clearly derived by using W and V.

It can be observed that in (3.25d) the sizes[1] of $\tilde{X}_\infty$ and $\Phi_\infty^{\tilde{x}}$ are the same and both are smaller than the size of $\breve{X}_\infty$. Considering (3.25a), (3.25b) and (3.25d), $\tilde{X}_\infty$ has the same size but generally different center with $\Phi_\infty^{\tilde{x}}$.

3.4.3 Relationship in Terms of Residuals

It is known that, for the interval observer-based method, the residual zonotopes defined in (3.12) can be rewritten as

$$R_k^{io} = C\tilde{X}_k \oplus \{\eta_k\} \oplus (-V), \tag{3.26}$$

[1]The size of a zonotope is used to describe the volume of the zonotope. However, one has difficulties to compute the volume of a zonotope. Thus, in this dissertation, the size is indirectly described by the interval hull width of the zonotope as in Definition 2.14.

where R_k^{io} is always bounded by its bounding set $\check{R}_k^{io}$ given in (3.22), as long as the initial condition $\tilde{X}_0 \subseteq \check{X}_0$ holds (i.e., $R_0^{io} \subseteq \check{R}_0^{io}$). As per (3.14) and (3.26), the center $r_k^{io,c}$ and segment matrix H_k^{io} of R_k^{io} have the expressions

$$r_k^{io,c} = C\tilde{x}_k^c + \eta_k - \eta^c, \tag{3.27a}$$

$$H_k^{io} = [C\tilde{H}_k^x \quad H_{\bar{\eta}}]. \tag{3.27b}$$

Similarly, for the invariant set-based method, by substituting (3.23) and (3.24) into (3.7), the residual set R_j^{is} corresponding to RPI sets can be obtained as

$$R_j^{is} = C\Phi_j^{\tilde{x}} \oplus V, \tag{3.28}$$

where j denotes the number of iterative steps indicated in Proposition 2.1, which does not mean the time instant. Similarly, the center $r_j^{is,c}$ and segment matrix H_j^{is} of R_j^{is} can be obtained as

$$r_j^{is,c} = C\xi_j^c + \eta^c, \tag{3.29a}$$

$$H_j^{is} = [CH_j^{\tilde{x}} \quad H_{\bar{\eta}}]. \tag{3.29b}$$

According to (3.25), (3.27b) and (3.29b), as k and j tend to infinity, the size of R_k^{io} converges to that of the smallest residual set R_∞^{is} corresponding to the mRPI set $\Phi_\infty^{\tilde{x}}$ of the dynamics (3.6). It can also be observed that the centers of R_∞^{io} and R_∞^{is} are generally different but have relationship

$$r_\infty^{io,c} + r_\infty^{is,c} = C[I - (A - LC)]^{-1}(\omega_\infty - L\eta_\infty) + \eta_\infty,$$

where, since ω_∞ and η_∞ are bounded, $r_\infty^{io,c} + r_\infty^{is,c}$ is also bounded. This implies that, as k tends to infinity, R_∞^{io} will be a set that has the same size but generally different center with R_∞^{is}. Residual zonotopes estimated by the interval observer have bounding zonotopes, (i.e., if $R_0^{io} \subseteq \check{R}_0^{io}$, then $R_k^{io} \subseteq \check{R}_k^{io}$ for all $k \geq 0$). But, one cannot assure that, at infinity, R_∞^{is} is bounded by $\check{R}_\infty^{io}$. However, if one can assure $\Phi_\infty^{\tilde{x}} \subseteq \check{X}_\infty$, then R_∞^{is} can be bounded by $\check{R}_\infty^{io}$. Thus, by comparing (3.15) with (3.21), it can be observed that the difference of $\tilde{X}_\infty$ and $\check{X}_\infty$ is from the term $-L\eta_k + \omega_k$ as in (3.15a). Thus, at infinity, considering (3.25a) and (3.25c), a condition such that $R_\infty^{is} \subseteq \check{R}_\infty^{io}$ can be obtained as $\omega^c - L\eta^c \in W \oplus L(-V) \oplus \{-(\omega^c - L\eta^c)\}$, i.e.,

$$2(\omega_c - L\eta_c) \in W \oplus L(-V). \tag{3.30}$$

3.4.4 Brief Discussions

Based on the residual forms (3.5) and (3.12) for the interval observer-based and the invariant set-based approaches, the relationship of both FD approaches is briefly summarized as follows:

- The principles of both FD approaches are similar. For the invariant set-based approach, the invariant set is fixed and determined off-line but the residual is obtained in real time, while, for the interval observer-based approach, the origin $\mathbf{0}$ is fixed but residual zonotopes are computed on-line.
- As k tends to infinity, the size of residual zonotopes estimated by the interval observer converges to that of the smallest residual set R_{∞}^{is}.
- The center of R_{∞}^{io} has a mathematical relationship with that of R_{∞}^{is}.
- As long as the corresponding initial condition is satisfied, R_k^{io} is always bounded by $\check{R}_k^{io}$. Although one cannot draw the same conclusion for R_k^{is} and $\check{R}_k^{io}$, R_{∞}^{is} can also be bounded by $\check{R}_{\infty}^{io}$ under the condition (3.30).

Remark 3.5. *Both FD approaches detect faults by testing consistency between the current behaviors of the system and the nominal behaviors from the nominal system model. Thus, once interval vectors estimated by the nominal interval observer do not include the origin or the residual exits the healthy residual set, it is considered that the system has become faulty, which means that the aforementioned discussions are generally suitable for all detectable*[1] *faults by both approaches. Note that the established relationship can also be extended to the case of faulty operation, as long as both interval observers and invariant sets are designed and constructed based on the same model of the faulty system.*

3.5 Comparison of Invariant Sets and Interval Observers

3.5.1 Computational Complexity

The computational complexity of the interval observer-based approach is mainly from the type of containment sets to propagate the effect of uncertainties throughout the system model and the algorithms to compute intervals. In [49], the algorithms to implement interval observers are classified into the *region-based* and *trajectory-based* algorithms. Generally, the former has lower computational complexity than the latter and different types of containment sets require different computational efforts. Besides, the interval observer-based approach estimates state and output sets on-line, which increases computational burden.

For the invariant set-based approach, since the key invariant set is computed off-line, the computational complexity of invariant sets does not play a decisive role in the complexity of the approach. During the runtime of the invariant set-based approach, its computational cost reduces to simple on-line set membership testing, i.e., check

[1] For the notion of fault detectability and isolability, one can turn to books related to this topic such as [5].

whether or not the residual exits its fixed healthy set. Thus, comparatively, the invariant set-based approach has much lower computational burden.

Generally, the invariant set-based approach has lower computational complexity than the interval observer-based approach. However, when using zonotopes to implement interval observers, the requirements of computational resources by interval observers is already satisfactory for considerable applications.

3.5.2 Conservatism in Fault Detection

For the invariant set-based approach, the conservatism comes mainly from the size of invariant sets. According to [44], invariant sets for on-line FD can approximate the mRPI set of the same dynamics with an arbitrarily expected precision. This precision can be assigned in advance. If a sufficiently small invariant set is obtained, the conservatism could be reduced to some extent. It is clear that the best invariant set for FD is the mRPI set. However, generally, it is impossible to obtain the mRPI set. Instead, the mRPI set can only be approximated by other bigger invariant sets, which implies a degree of conservatism.

Additionally, for the invariant set-based approach, there mainly exist two dynamic processes. The first one is the residual movement from the outside of the invariant set to the inside while the second one is the opposite. The former corresponds to the initial transient-state process or system-recovery/FI process from a mode to another mode, while the latter corresponds to the FD process. This chapter focuses on the initial transient-state and steady-state FD processes and omits system recovery/FI processes. In reality, since the invariant set is fixed and computed off-line but used on-line, it has a fixed size and does not have adjustable flexibility on-line. Thus, it is possible that the system initial condition is outside the healthy invariant set, which results in that the invariant set-based approach loses its effectiveness to detect faults during the initial and transit processes. Theoretically, the interval observer can reduce this conservatism by arbitrarily assigning its initial set under the physical constraints of the system to contain the initial condition for the initial and transient FD processes. Besides, during FD, one has to use an invariant set with a fixed size bigger than that of the mRPI set. But, for the interval observer, because of on-line propagation, the sizes of estimated sets will be able to approach that of the mRPI set as much as possible as time elapses. Thus, after sufficiently long operating time, the sizes of sets from interval observers should be smaller than that of the invariant set, which should be better for FD.

It can be observed that both approaches have their advantages and disadvantages. Interval observers can provide system dynamic information during the whole process including the initial, transient and steady state, which means that they can detect faults during the whole process but with higher complexity because of on-line set computation. Comparatively, invariant sets mainly describe the system behaviors at steady state, which are mainly used for steady-state FD but with lower complexity because of

off-line invariant set construction. Thus, generally speaking, from FD point of view, the interval observer-based approach should be less conservative, while from computational point of view, the invariant set-based approach is less complex. Ideally, if they can be used jointly, it is possible to use them to mitigate their respective disadvantages and make use of their respective advantages. This point motivates the following research of this dissertation.

3.6 Illustrative Example

A discrete-time dynamics under the effect of sensor faults is used to illustrate the results related to both FD approaches, whose model is given as

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k, \\ y_k &= G_i C x_k + \eta_k, \end{aligned}$$

where G_i is a diagonal matrix modelling the i-th sensor mode ($i \in \{0, 1\}$). G_0 is the identity matrix modelling the healthy mode and G_1 models a faulty mode. An interval observer as in (3.9) is designed to monitor the plant. The residual zonotopes and the residual for both FD approaches are defined as (3.5) and (3.12), respectively. The parameters of this example are given as:

- Model matrices: $A = \begin{bmatrix} 0.867 & -1.234 \\ 0.01 & 1 \end{bmatrix}, B = \begin{bmatrix} 0.01 & 1 \\ 1 & 0.01 \end{bmatrix}, C = \begin{bmatrix} 0.5 & 0 \\ 0 & 1.5 \end{bmatrix}.$
- Disturbances: $\bar{w} = \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T, w^c = \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T.$
- Measurement noises: $\bar{\eta} = \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T, \eta^c = \begin{bmatrix} 0.5 & 0.5 \end{bmatrix}^T.$
- Observer gain and fault magnitude: $L = \begin{bmatrix} 0.533 & -0.823 \\ 0.02 & 0.2 \end{bmatrix}, G_1 = \begin{bmatrix} 0.95 & 0 \\ 0 & 1 \end{bmatrix}.$
- Input set[1]: $u^c = \begin{bmatrix} 2 \\ 2 \end{bmatrix}, H_u = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.2 \end{bmatrix}.$
- Initial conditions: $x_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \hat{X}_0 = \begin{bmatrix} 0.1 \\ 0.1 \end{bmatrix} \oplus \begin{bmatrix} 2 & 0 & 2 \\ 0 & 2 & 2 \end{bmatrix} \mathbb{B}^3.$
- Sampling time: 0.01s

For the invariant set-based approach, one can compute an initial invariant set for the dynamics of the estimation error as in (3.6). Then one can use this initial invariant set

[1]This example considers two inputs. The input set is given as a zonotope, whose center and segment matrix are denoted as u^c and H_u, respectively.

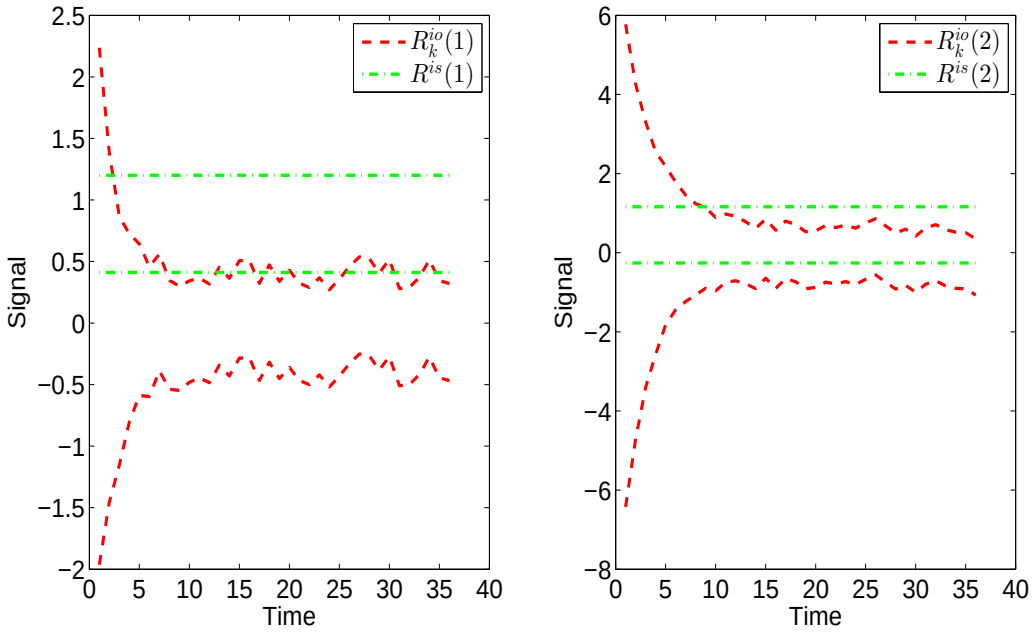


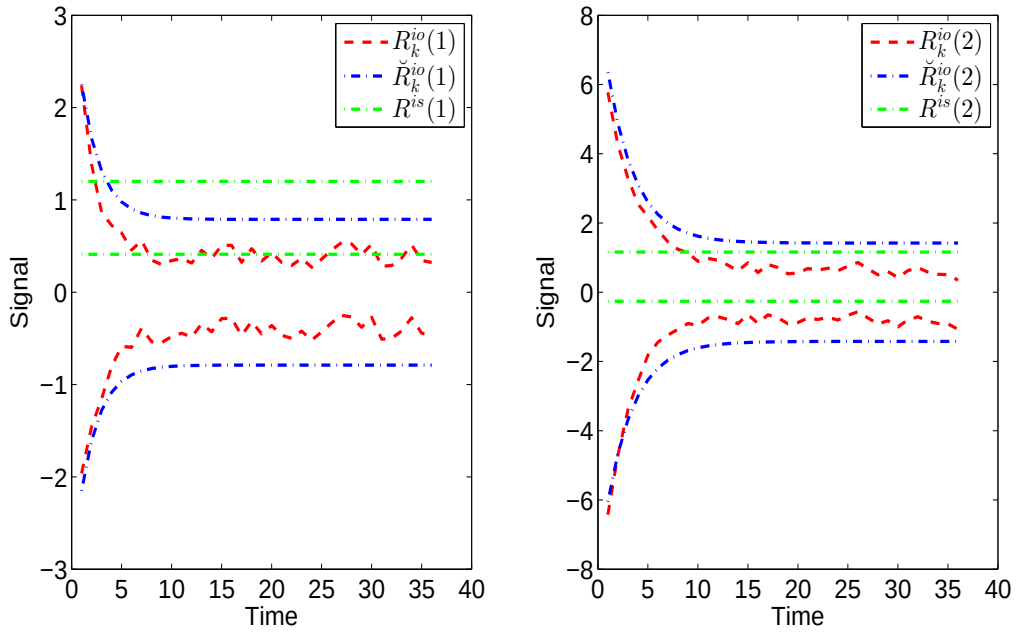
Figure 3.2: Relationship in terms of set sizes

to iterate the corresponding set-based description of the dynamics thirty steps to obtain another invariant set of the dynamics, which can sufficiently approaches the mRPI set. Based on this invariant set, the corresponding healthy residual set can be constructed with the residual equation as in (3.5). The interval hull of this thirty-step residual set is computed off-line as $\square R_{30}^{is} = ([0.4114, 1.2005], [-0.26, 1.1])^T$, whose size is denoted as a vector $width(R_{30}^{is}) = \begin{bmatrix} 0.7891 & 1.42 \end{bmatrix}^T$. In the sequel, this residual set is used to illustrate the established relationship. Note that since the illustrative example has two dimensions, the interval hull (or interval vector) and its width (or vector) also includes two components.

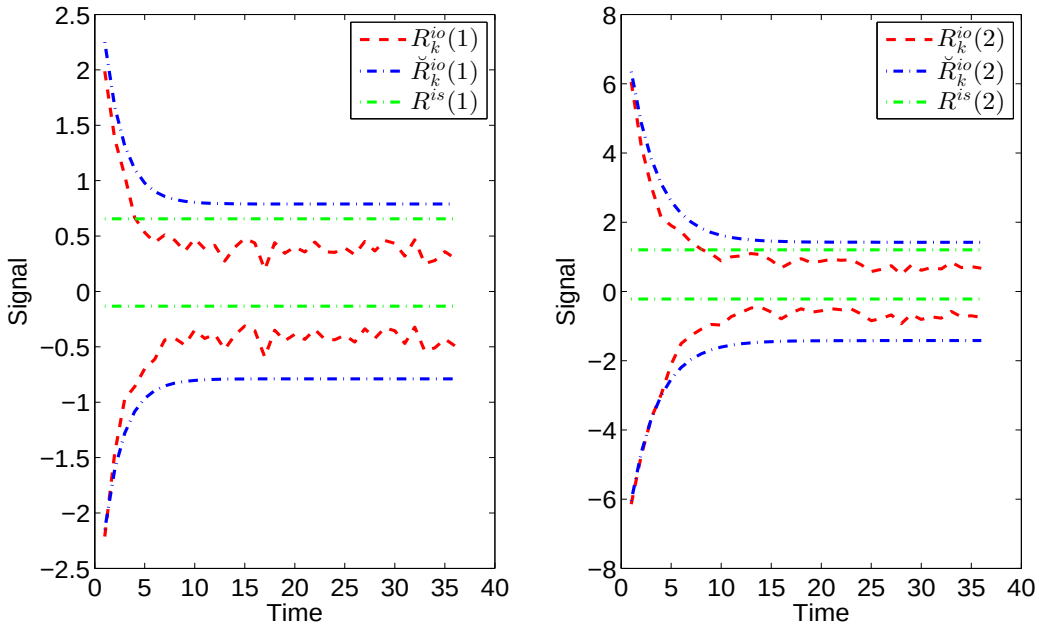
Remark 3.6. *For comparison, instead of directly using zonotopes, one uses the interval hull of zonotopes. In this case, for each dimension of the residual (or residual zonotope), an interval can be obtained to bound the component in that dimension.*

3.6.1 Relationship in Terms of Set Sizes

The relationship between residual zonotopes and the healthy residual set is shown in Figure 3.2. It can be observed that residual zonotopes do not converge to the residual set but their sizes converge to that of the residual set. In Figure 3.2, after

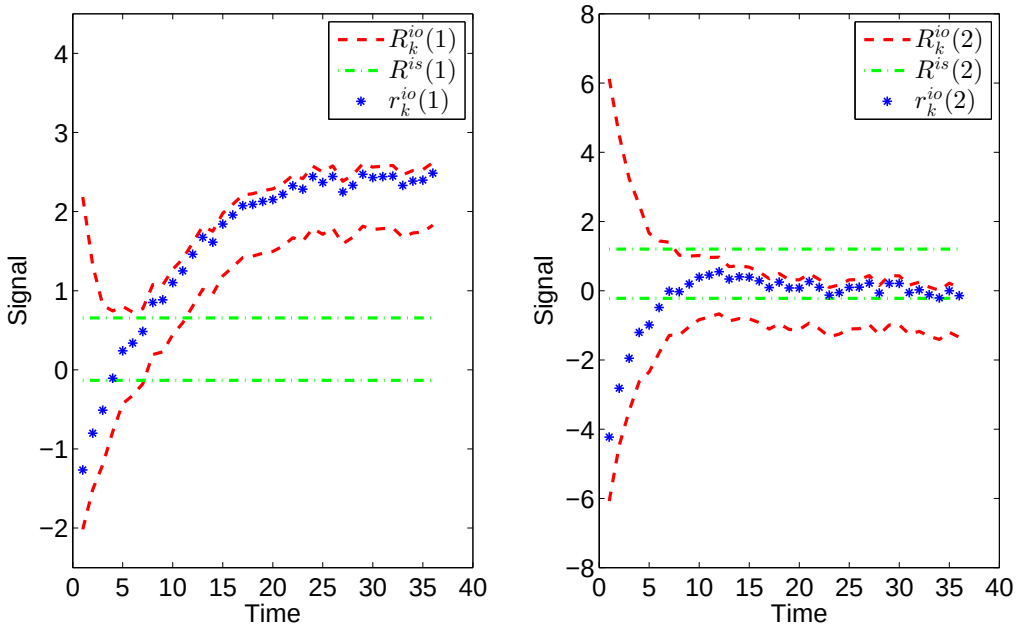


(a) Residual set outside bounding intervals

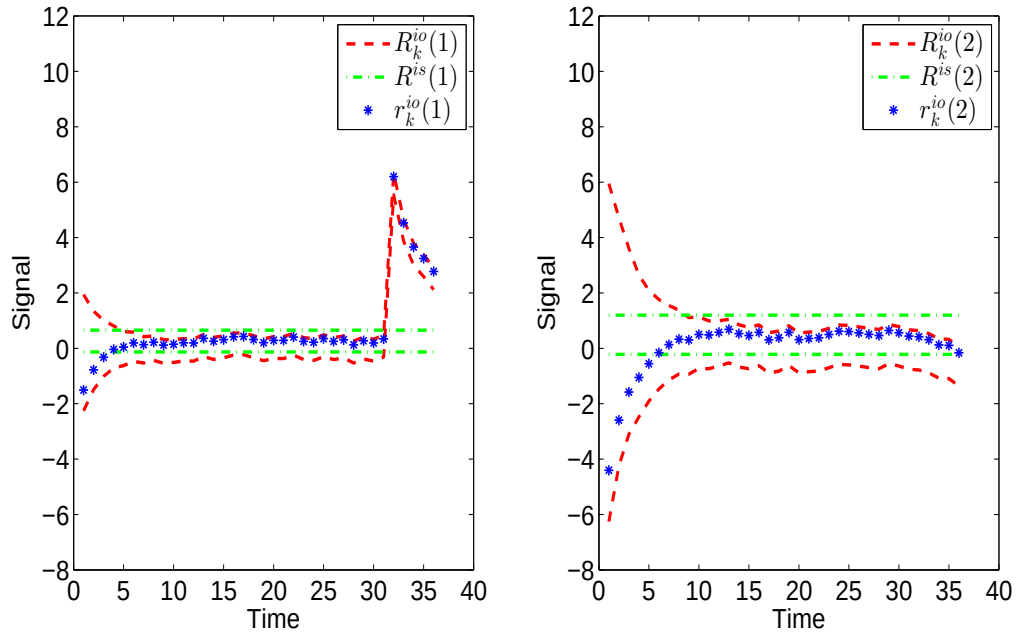


(b) Residual set inside bounding intervals

Figure 3.3: Relationship in terms of bounds



(a) FD in initial transient state



(b) FD in steady state

Figure 3.4: Two approaches in FD

twenty-step on-line propagation, the size of residual zonotopes approximately reaches $\begin{bmatrix}0.7891 & 1.42\end{bmatrix}^T$, which is consistent with that of the residual set.

Remark 3.7. *In the figures, $R_k^{io}(1)$, $R^{is}(1)$, $\check{R}_k^{io}(1)$ and $r_k^{io}(1)$ and $R_k^{io}(2)$, $R^{is}(2)$, $\check{R}_k^{io}(2)$ and $r_k^{io}(2)$ are the first and second components of R_k^{io}, R^{is}, $\check{R}_k^{io}$ and r_k^{io}, respectively.*

3.6.2 Relationships in Terms of Bounds

Figure 3.3 shows the relationship among the residual set, the residual zonotopes and their bounds, where residual zonotopes are always bounded by their bounds, while the residual set is not always bounded by the same bounds. Note that, in Figure 3.3(a), based on the aforementioned parameters, the residual set is not bounded by the same bounds. Instead, in Figure 3.3(b), based on a new center $\eta^c = \begin{bmatrix}0.1 & 0.1\end{bmatrix}^T$ that satisfies (3.30), the residual set is always bounded by the same bounds.

3.6.3 Relationships in Transient and Steady Fault Detection

In Figure 3.4, the two approaches are used to detect the same fault during the initial-state and steady-state processes, respectively. In Figure 3.4(a), the fault occurs at time instant 3 (transient state) and in Figure 3.4(b) the fault occurs at time instant 30 (steady state). It can be observed that the interval observer can detect the fault both at initial state and steady state by testing that the inclusion (3.13) is violated while the invariant set-based approach can only detect the fault at steady state by testing the inclusion (3.8). At transient state, if the initial value is outside the residual set, even though a fault occurs, the invariant set-based approach cannot make a decision for fault occurrence. Comparatively, for the interval observer, its initial set can be arbitrarily assigned as big as possible to contain the initial value, thus, once a violation of (3.13) is detected, it implies fault occurrence. This shows the advantage of the interval observer-based approach in transient-state FD and the principle similarity of the two approaches in steady-state FD. In Figure 3.4, the center of the noise set is given as $\eta^c = \begin{bmatrix}0.1 & 0.1\end{bmatrix}^T$.

3.6.4 Comparison of Computational Complexity

The invariant set-based approach implements FD by only testing whether or not the residual is inside its healthy set, while the interval observer-based approach performs FD by estimating the state and output sets on-line. As mentioned in this chapter, the former has less computational complexity than the latter. However, in order to intuitively show their complexity, one applies the two FD approaches into this example. With a simulation time of 10000 steps, for the invariant set-based approach,

the CPU time is around 0.145110 seconds, while for the interval observer-based approach, the CPU time is around 0.691144 seconds. This shows that the invariant set-based approach has very obvious advantage in terms of computational complexity. The computer type model for this testing is HP Elitebook 6930p (processor: Inter(R) Core(TM)2 Duo CPU p8700, 2.53GHz; RAM: 4.00GB; 64-bit operating system).

Remark 3.8. *One should use different examples to show different relationships of interval observers and invariant sets. But, in this chapter, without loss of generality, one uses the same example with some different parameters to show all the aforementioned relationships for brevity. For example, in Figures 3.3(b) and 3.4, one changes the center of the set V of measurement noises, while for the results of the other figures, one uses the original parameters given at the beginning of this section.*

Remark 3.9. *Theoretically, for a system, as long as its invariant sets can be constructed and its interval observers can be computationally feasible, one can use invariant sets and interval observers for its fault diagnosis. Realistically, invariant set construction and interval observer implementation depend on the complexity of the system such as the number of inputs, states and outputs. However, this is already out of the scope of this dissertation and could be a separate topic of the future research.*

3.7 Summary

This chapter analyzes the interval observer-based and the invariant set-based FD approaches. The former can provide the system information during the whole process with higher computational complexity, while the latter focuses more on the steady-state behaviors of the system with lower computational complexity. Both interval observers and invariant sets have their own advantages and disadvantages, respectively. The next chapters are to explore the possibility of combining both approaches in fault diagnosis.

Chapter 4

Actuator-fault Detection and Isolation using Set-based Methods

This chapter proposes an actuator FDI approach based on the results obtained in the previous chapter. This FDI approach is based on a bank of interval observers, each of which is designed to match a healthy or faulty actuator mode. In order to guarantee FDI, a collection of invariant set-based FDI conditions are established. Under these FDI conditions, all considered actuator faults can be detected and then isolated. A continuous stirred-tank reactor (CSTR) example is used to illustrate the effectiveness of the proposed FDI approach.

4.1 Introduction

Interval observers, as one of set-theoretic approaches, are well-known for robust FD, which consists in propagating the effect of uncertainties through system models to generate real-time output intervals [20, 36, 39]. Provided that the system is healthy, the output vectors should be inside their intervals estimated by the interval observer based on the system nominal model. When the system is affected by faults, once the current outputs violate their intervals, the FD task will be triggered. Regarding FI, interval observers generally turn to other FI techniques. So far, few works have been done for the FI application of interval observers, especially for the interval observer-based FI with FI guarantees.

The objective of this chapter is to propose an interval observer-based FDI approach for actuator faults, in which both FD and FI are implemented by means of interval observers and without relying on other FI techniques. This chapter is based on the works [65, 67] and follows the system framework shown in Figure 4.1. In this chapter, the design of interval observers is based on the Luenberger-observer structure. The uncertainties (disturbances, bias and noises, etc) and unknown but bounded faults are

considered. In order to obtain a balance of computational precision and complexity, the proposed approach uses zonotopes as its bounding set to propagate the effect of uncertainties on the plant.

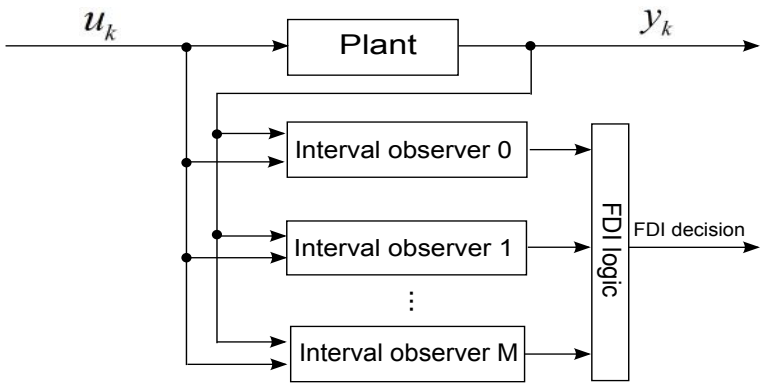


Figure 4.1: Actuator FDI scheme

This approach has three main contributions. First, the proposed approach provides a novel perspective to the FI application of interval observers by combining interval observers with invariant sets. Second, by using interval observers, the proposed method can deal with unknown but bounded actuator faults. Third, this technique can detect and isolate actuator faults during the transition induced by faults with FDI guarantees.

4.2 Problem Formulation

4.2.1 Plant Models

This chapter considers the linear discrete time-invariant plant under the effect of actuator faults, which is modelled as

$$x_{k+1} = Ax_k + BF_i u_k + \omega_k, \tag{4.1a}$$
$$y_k = Cx_k + \eta_k, \tag{4.1b}$$

where the matrix F_i ($i \in \mathbb{I} = \{0, 1, \cdots, M\}$ models a finite range of healthy or faulty actuator modes important to system performance/safety)[1] is a $p \times p$ diagonal matrix modelling the i-th actuator mode and all the other parameters/variables in (4.1) respect the corresponding definitions as in (3.1).

F_0 is the identity matrix with suitable dimensions and describes the healthy actuator mode, and F_i ($i \neq 0$) models the fault-affected system. The diagonal elements of F_i

[1] A system mode characterizes the system as being under a certain dynamics, which corresponds to either healthy or faulty behaviors.

($i \neq 0$) belong to the interval [0, 1], where an element taking the value 0 or 1 represents the complete outage or health of the corresponding actuator, respectively, while taking a value inside (0, 1) denotes the partial performance degradation of the corresponding actuator. Besides, the uncertainties ω_k and η_k are unknown but bounded by known sets W and V as defined in (3.2).

Assumption 4.1. *The pairs (A, BF_i) for all $i \in \mathbb{I}$ are stabilizable and the pair (A, C) is detectable.*

Remark 4.1. *The scheme in Figure 4.1 is not a closed-loop system, which does not explicitly consider the effect of inputs on the system stability. Thus, for the actuator FDI approach proposed in this chapter, the system stability assumption should be the first priority under Assumption 4.1.*

Assumption 4.2. *In the i-th actuator-fault mode, F_i is bounded by an interval matrix $\mathbf{F_i}$ (i.e., $F_i \in \mathbf{F_i}$), where F_i (the actual magnitude of the i-th fault) is unknown but $\mathbf{F_i}$ (the bound of the considered magnitude of the i-th fault) is given and known.*

Remark 4.2. *A fault occurrence (or mode switching) indicates a change from F_i to F_j ($i \neq j$) in (4.1). Since the actual actuator-fault magnitude is unknown, when the system is in the operation of the i-th mode, F_i can be any value inside its bound $\mathbf{F_i}$, which implies that F_i can be constant or time-varying with any profile.*

4.2.2 Interval Observers

Interval observers use the inputs and outputs to estimate the state and output sets. The interval observer corresponding to the healthy operation is firstly introduced to explain the general design of interval observers, which is further employed for the description of the rest of interval observers.

4.2.2.1 Interval Observer for Healthy Mode

Based on (4.1), the healthy interval observer with Luenberger structure

$$\hat{x}_{k+1} = A\hat{x}_k + BF_0u_k + L_0(y_k - \hat{y}_k) + \breve{\omega}_k, \tag{4.2a}$$
$$\hat{y}_k = C\hat{x}_k + \breve{\eta}_k, \tag{4.2b}$$

is designed to monitor the system, where L_0 is the observer gain matrix. In the Luenberger-observer structure (4.2), the uncertain variables $\breve{\omega}_k$ and $\breve{\eta}_k$ are used to describe the effect of ω_k and η_k in the plant (4.1) on the state and output estimations $\hat{x}_k$ and $\hat{y}_k$, respectively. The uncertain variables $\breve{\omega}_k$ and $\breve{\eta}_k$ are different from ω_k and η_k but are defined to have the same bounds, respectively (i.e., $\breve{\omega}_k \in W$ and $\breve{\eta}_k \in V$). By

substituting (4.2b) into (4.2a), (4.2) can be equivalently transformed into

$$\hat{x}_{k+1} = (A - L_0C)\hat{x}_k + BF_0u_k + L_0y_k - L_0\check{\eta}_k + \check{\omega}_k, \tag{4.3a}$$

$$\hat{y}_k = C\hat{x}_k + \check{\eta}_k. \tag{4.3b}$$

While acknowledging that the actual noises are not measurable but manipulated set-wise, $\check{w}_k$ and $\check{\eta}_k$ respectively emulate ω_k and η_k from (4.1) and are used to cover the effect of ω_k and η_k on the state and output estimations from (4.2). In the healthy mode, the healthy interval observer able to estimate the state and output sets that bound the system states and outputs is obtained as

$$\hat{X}^0_{k+1} = (A - L_0C)\hat{X}^0_k \oplus \{BF_0u_k\} \oplus \{L_0y_k\} \oplus (-L_0)V \oplus W, \tag{4.4a}$$

$$\hat{Y}^0_k = C\hat{X}^0_k \oplus V \tag{4.4b}$$

by substituting the sets W and V bounding $\check{w}_k$ and $\check{\eta}_k$ into (4.3), where $\hat{X}^0_k$ and $\hat{Y}^0_k$ are the estimated state and output sets at time instant k, respectively, and L_0 is chosen to assure that $A - L_0C$ is a Schur matrix, which is always possible under Assumption 4.1.

Remark 4.3. *The interval observer is a set-based observer that converges under the Schur-matrix hypothesis for the matrix $A - L_0C$ independent of the topology of the sets in the construction. Naturally, these properties are inherited in the case of zonotopic sets used in this chapter.*

Considering that W and V are zonotopes as in (3.3), zonotopes to bound the estimated outputs and states can be constructed by introducing zonotopic sets of $\check{\omega}_k$ and $\check{\eta}_k$ into the observer mapping (4.3) and using zonotope arithmetic at each time instant.

Assumption 4.3. *The initial state of the plant is denoted as x_0 and all interval observers are initialized by a common zonotopic set $\hat{X}_0$ such that $x_0 \in \hat{X}_0$ holds.*

Remark 4.4. *Although the initial set of each interval observer can be assigned differently, for brevity, one uses one initial set for the initialization of all interval observers.*

Remark 4.5. *Under Assumption 4.3, it is guaranteed that the current states and outputs are always bounded by the state and output zonotopes estimated by an interval observer whose internal model matches the current system mode.*

Since interval observers are based on zonotopes, the discussion is also based on zonotopes in the remaining of the chapter.

4.2.2.2 Interval Observers for Actuator-fault Modes

Similarly, the j-th interval observer matching the j-th actuator-fault mode ($j \neq 0$) is designed as

$$\hat{X}^j_{k+1} = (A - L_jC)\hat{X}^j_k \oplus \{B\mathbf{F_j}u_k\} \oplus \{L_jy_k\} \oplus (-L_j)V \oplus W, \tag{4.5a}$$

$$\hat{Y}^j_k = C\hat{X}^j_k \oplus V, \tag{4.5b}$$

where $\hat{X}_k^j$ and $\hat{Y}_k^j$ are the estimated state and output zonotopes at time instant k, respectively, and L_j is chosen to assure that $A - L_jC$ is a Schur matrix, which is guaranteed by Assumption 4.1.

Remark 4.6. *The gains of different interval observers are separately designed.*

Remark 4.7. *In Property 2.7, if H_k, $\mathbf{B}$ and u_k are zero, Property 2.7 will reduce to the computation of a zonotope to bound the multiplication of an interval matrix and a vector. In this case, by using the reduced result of Property 2.7, the term $\mathbf{F_j}u_k$ in (4.5) can be over-approximated by a zonotope whose center and segment matrix are $mid(\mathbf{F_j})u_k$ and $\frac{diam(\mathbf{F_j})}{2}u_k$, respectively.*

As per Remark 4.7, $\mathbf{F_j}u_k$ in (4.5) can be replaced by its zonotopic over-approximation. In this way, one can obtain a computable form of (4.5), i.e., an over-approximation of (4.5). Moreover, using zonotope manipulations, the obtained computable form of (4.5) can be equivalently split into the center-segment matrix description

$$\hat{x}_{k+1}^{j,c} = (A - L_jC)\hat{x}_k^{j,c} + B\,mid(\mathbf{F_j})u_k + L_jy_k - L_j\eta^c + w^c, \tag{4.6a}$$

$$\hat{H}_{k+1}^{j,x} = [(A - L_jC)\hat{H}_k^{j,x} \;\; B\frac{diam(\mathbf{F_j})}{2}u_k \;\; - L_jH_{\bar{\eta}} \;\; H_{\bar{\omega}}], \tag{4.6b}$$

$$\hat{y}_k^{j,c} = C\hat{x}_k^{j,c} + \eta^c, \tag{4.6c}$$

$$\hat{H}_k^{j,y} = [C\hat{H}_k^{j,x} \quad H_{\bar{\eta}}], \tag{4.6d}$$

where $\hat{x}_{k+1}^{j,c}$ and $\hat{y}_k^{j,c}$ are the centers of $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$, and $\hat{H}_{k+1}^{j,x}$ and $\hat{H}_k^{j,y}$ are the segment matrices of $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$, respectively.

For brevity, one uses the same notations $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ to denote the state and output set estimations of both (4.5) and (4.6). It can be observed that $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ corresponding to (4.6) are the over-approximations of $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ in (4.5), respectively, where the former is the particular implementation of interval observers while the latter is the theoretical expression of interval observers. Since only (4.6) is used to estimate state and output sets in the proposed approach, $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ used in the remaining of the chapter denote the state and output sets estimated by (4.6).

Remark 4.8. *Letting $j = 0$ in (4.6), the center $\hat{x}_{k+1}^{0,c}$ and segment matrix $\hat{H}_{k+1}^{0,x}$ of $\hat{X}_{k+1}^0$, and the center $\hat{y}_k^{0,c}$ and segment matrix $\hat{H}_k^{0,y}$ of $\hat{Y}_k^0$, corresponding to the healthy interval observer, can be accurately obtained.*

4.3 Residual Analysis

4.3.1 Residual Zonotopes

It is necessary to define a residual for the model-based FDI approach. Different from the traditional residual definition as a vector, the residual here is defined in terms of

zonotopes. According to (4.1), (4.4) and (4.6), the residual zonotope is defined as

$$\begin{aligned} R_k^{ij} &= \{y_k\} \oplus (-\hat{Y}_k^j) \\ &= \{Cx_k + \eta_k\} \oplus (-C\hat{X}_k^j) \oplus (-V) \\ &= C\{\{x_k\} \oplus (-\hat{X}_k^j)\} \oplus \{\eta_k\} \oplus (-V), \end{aligned} \tag{4.7}$$

where R_k^{ij} denotes the residual zonotope estimated by the j-th interval observer when the plant is in the i-th mode at time instant k. To obtain the set values of R_k^{ij}, the expression $\tilde{X}_k^{ij} = \{x_k\} \oplus (-\hat{X}_k^j)$ in (4.7) should be considered, which is derived as

$$\begin{aligned} \tilde{X}_k^{ij} &= \{x_k\} \oplus (-\hat{X}_k^j) \\ &= (x_k - \hat{x}_k^{j,c}) \oplus \hat{H}_k^{j,x} \mathbb{B}^{s_k^j}, \end{aligned} \tag{4.8}$$

where s_k^j represents the order of the zonotope $\tilde{X}_k^{ij}$. According to (4.1) and (4.6), at time instant $k+1$, using $\tilde{x}_{k+1}^{ij,c}$ and $\tilde{H}_{k+1}^{ij,x}$ to denote $x_{k+1} - \hat{x}_{k+1}^{j,c}$ and $\hat{H}_{k+1}^{j,x}$ as in (4.8), the center $\tilde{x}_{k+1}^{ij,c}$ and segment matrix $\tilde{H}_{k+1}^{ij,x}$ of $\tilde{X}_{k+1}^{ij}$ can be computed as

$$\tilde{x}_{k+1}^{ij,c} = (A - L_jC)\tilde{x}_k^{ij,c} + B(F_i - mid(\mathbf{F_j}))u_k - L_j(\eta_k - \eta^c) + (\omega_k - \omega^c), \tag{4.9a}$$

$$\tilde{H}_{k+1}^{ij,x} = \hat{H}_{k+1}^{j,x},$$

$$\hat{H}_{k+1}^{j,x} = [(A - L_jC)\hat{H}_k^{j,x} \;\; B\frac{diam(\mathbf{F_j})}{2}u_k \;\; -L_jH_{\bar{\eta}} \;\; H_{\bar{\omega}}]. \tag{4.9b}$$

By substituting (4.8) into (4.7), the residual zonotope can be rewritten as

$$R_k^{ij} = C\tilde{X}_k^{ij} \oplus \{\eta_k\} \oplus (-V). \tag{4.10}$$

4.3.2 Adaptive Bounds for Residual Zonotopes

Substituting $\mathbf{F_i}$, W and V into (4.9a) to respectively replace F_i, ω_k and η_k, one can obtain a zonotope $\check{X}_{k+1}^{ij}$ to bound $\tilde{X}_{k+1}^{ij}$ described by (4.8) and (4.9). Moreover, the center $\check{x}_{k+1}^{ij,c}$ and segment matrix $\check{H}_{k+1}^{ij,x}$ of $\check{X}_{k+1}^{ij}$ can be derived as

$$\check{x}_{k+1}^{ij,c} = (A - L_jC)\check{x}_k^{ij,c} + Bmid(\mathbf{F_i})u_k - Bmid(\mathbf{F_j})u_k, \tag{4.11a}$$

$$\check{H}_{k+1}^{ij,x} = [(A - L_jC)\check{H}_k^{ij,x} \;\; B\frac{diam(\mathbf{F_i})}{2}u_k \;\; B\frac{diam(\mathbf{F_j})}{2}u_k \;\; L_jH_{\bar{\eta}} \;\; -L_jH_{\bar{\eta}} \;\; H_{\bar{\omega}} \;\; -H_{\bar{\omega}}]. \tag{4.11b}$$

Using Remark 4.7 and zonotope manipulations, an equivalent compact form of (4.11) can be derived as

$$\check{X}_{k+1}^{ij} = (A - L_jC)\check{X}_k^{ij} \oplus B\check{U}_i \oplus B(-\check{U}_j) \oplus L_j(-V) \oplus W \oplus L_jV \oplus (-W), \tag{4.12}$$

where the sets $\check{U}_i$ and $\check{U}_j$ are zonotopes, which are computed by

$$\check{U}_i = \{mid(\mathbf{F_i})u_k\} \oplus \frac{diam(\mathbf{F_i})}{2} u_k \mathbb{B}^{s_{\check{u}_i}}, \tag{4.13a}$$

$$\check{U}_j = \{mid(\mathbf{F_j})u_k\} \oplus \frac{diam(\mathbf{F_j})}{2} u_k \mathbb{B}^{s_{\check{u}_j}}, \tag{4.13b}$$

where $s_{\check{u}_j}$ and $s_{\check{u}_j}$ are the orders of $\check{U}_j$ and $\check{U}_j$, respectively.

Proposition 4.1. *If $\tilde{X}_{k^*}^{ij} \subseteq \check{X}_{k^*}^{ij}$ holds, $\tilde{X}_k^{ij}$ will always be bounded by $\check{X}_k^{ij}$ for all $k > k^*$.*

Proof : Since (4.11) is obtained by substituting the bounds of F_i, ω_k and η_k into (4.9), if, at time instant k^*, $\tilde{X}_{k^*}^{ij} \subseteq \check{X}_{k^*}^{ij}$ holds, then after k^*, the inclusion will always hold. □

According to Proposition 4.1, by introducing $\check{X}_k^{ij}$ and V into (4.10), a computable bound for R_k^{ij} can be obtained as

$$\check{R}_k^{ij} = C\check{X}_k^{ij} \oplus V \oplus (-V). \tag{4.14}$$

4.3.3 Static Bounds for Residual Zonotopes

In (4.12), the adaptive bound $\check{X}_k^{ij}$ of $\tilde{X}_k^{ij}$ always tracks the evolution of control inputs. Since FDI conditions of the proposed approach are established by using fixed steady sets, in order to establish FDI conditions, it is necessary to obtain a static bound for $\tilde{X}_k^{ij}$ (not affected by the evolution of inputs).

Assumption 4.4. *The input vector u_k of the plant is bounded by*

$$U = \{u \in \mathbb{R}^p : \ |u - u^c| \leq \bar{u}, u^c \in \mathbb{R}^p, \bar{u} \in \mathbb{R}^p\},$$

where the vectors u^c and $\bar{u}$ are constant. Furthermore, the set U can be rewritten as a zonotope $U = u^c \oplus H_{\bar{u}}\mathbb{B}^p$, where $H_{\bar{u}} \in \mathbb{R}^{p\times p}$ is a diagonal matrix with the main diagonal being composed of $\bar{u}$.

By replacing u_k in (4.11) with its bound U, one can obtain a static bound denoted as $\check{X}_{k+1}^{ij}$ for both $\tilde{X}_{k+1}^{ij}$ and $\check{X}_{k+1}^{ij}$ and the set-based dynamics of $\check{X}_{k+1}^{ij}$ are expressed as

$$\check{X}_{k+1}^{ij} = (A - L_jC)\check{X}_k^{ij} \oplus B\check{U}_i \oplus B(-\check{U}_j) \oplus L_j(-V) \oplus W \oplus L_jV \oplus (-W), \tag{4.15}$$

where, according to Properties 2.6 and 2.7 in Chapter 2, the sets $\check{U}_i$ and $\check{U}_j$ are zonotopes, which are computed by

$$\check{U}_i = \{mid(\mathbf{F_i})u_c\} \oplus [seg(\diamond(\mathbf{F_i}H_{\bar{u}})) \quad \frac{diam(\mathbf{F_i})}{2} u_c] \mathbb{B}^{s_{\check{u}_i}}, \tag{4.16a}$$

$$\check{U}_j = \{mid(\mathbf{F_j})u_c\} \oplus [seg(\diamond(\mathbf{F_j}H_{\bar{u}})) \quad \frac{diam(\mathbf{F_j})}{2} u_c] \mathbb{B}^{s_{\check{u}_j}}, \tag{4.16b}$$

where $s_{\check{u}_i}$ and $s_{\check{u}_j}$ denote the orders of the zonotopes $\check{U}_i$ and $\check{U}_j$, respectively. Thus, from the set-theoretic point of view, one can define an equivalent dynamics for (4.15), which is presented as

$$\check{x}_{k+1}^{ij} = (A - L_j C)\check{x}_k^{ij} + B\check{u}_{i_k} - B\check{u}_{j_k} - L_j\eta_k + \check{\omega}_k + L_j\check{\eta}_k - \omega_k, \tag{4.17}$$

where $\check{u}_{i_k} \in \check{U}_i$, $\check{u}_{j_k} \in \check{U}_j$, $\check{\eta}_k \in V$ and $\check{\omega}_k \in W$ hold.

As per the notions of RPI and mRPI sets, an RPI set for (4.17) can be computed and further written in the zonotopic form. Moreover, using the RPI set as an initial set for (4.15), after a finite number of iterations, an RPI approximation (denoted as $\mathring{X}^{ij}$) with an arbitrarily expected precision to the mRPI set of (4.17) can be computed. Since the mRPI set is the limit set of (4.15), as long as the precision of $\mathring{X}^{ij}$ is satisfactory, $\mathring{X}^{ij}$ can reliably replace the use of the mRPI set.

In the proposed approach, for each mode, the corresponding interval observer is designed according to the system mode model. By substituting $\check{X}_k^{ij}$ in (4.15) into (4.10), a static bound $\check{R}_k^{ij}$ for both R_k^{ij} and $\check{R}_k^{ij}$ can be obtained as

$$\check{R}_k^{ij} = C\check{X}_k^{ij} \oplus V \oplus (-V). \tag{4.18}$$

Remark 4.9. *Two different residual-related sets $\check{R}_k^{ij}$ and $\check{R}_k^{ij}$ are considered in the proposed approach. $\check{R}_k^{ij}$ and $\check{R}_k^{ij}$ as the two different bounds of R_k^{ij} have different uses, i.e., $\check{R}_k^{ij}$ is used for the on-line FI during the transition while $\check{R}_k^{ij}$ is used to establish FDI conditions. This will be elaborated in the following contents.*

Since the set $\mathring{X}^{ij}$ is an RPI approximation of the mRPI set $\check{X}_\infty^{ij}$, one can obtain a suitable approximation $\mathring{R}_\infty^{ij}$ for $\check{R}_\infty^{ij}$, which is expressed as

$$\mathring{R}_\infty^{ij} = C\mathring{X}^{ij} \oplus V \oplus (-V). \tag{4.19}$$

In Section 4.3, when $i = 0$ and $j = 0$, the relevant conclusions reduce to the case corresponding to the healthy interval observer under the healthy mode.

4.4 Fault Detection and Isolation Conditions

This section establishes FDI conditions for the proposed approach at steady state by using the static bound of residual zonotpes and the notion of invariant sets.

4.4.1 Theoretical Conditions

For the proposed approach, the theoretical FDI conditions are established by determining the dynamic behaviors of the system at infinity. As k tends to infinity, a collection

of guaranteed FDI conditions can be established using the static residual-bounding zonotopes $\breve{R}_{\infty}^{ij}$ as indicated in (4.18).

Theorem 4.1. *Given the plant* (4.1) *and a bank of interval observers* (4.4) *and* (4.5)*, for any mode i, if the static residual-bounding zonotopes corresponding to interval observers satisfy*

$$\mathbf{0} \in \breve{R}_{\infty}^{ii} \text{ and } \mathbf{0} \notin \breve{R}_{\infty}^{ij},\ j \neq i,\ i,\ j \in \mathbb{I}, \tag{4.20}$$

once a considered mode occurs, the detection and isolation of the mode can be guaranteed as the system converges to the steady state of the mode.

Proof : The proof includes three parts. The first one is to prove that (4.20) provides asymptotic FDI conditions. The second one focuses on the dynamic behaviors of the static residual-bounding zonotopes at infinity, i.e., $\breve{R}_{\infty}^{ij}$ translates the behaviors of the plant at steady state, which guarantees FDI. The third one is to prove that (4.20) guarantees FDI during the transition induced by mode switching.

- The satisfaction of (4.20) implies that only residual zonotopes estimated by the interval observer matching the current mode contain the origin $\mathbf{0}$ at infinity while residual zonotopes, estimated by the interval observers not matching the current mode, exclude $\mathbf{0}$ at infinity. Thus, (4.20) guarantees that the considered modes satisfying the theorem are detectable and isolable.

- Without loss of generality, the following proof is based on the relevant set-based dynamics. (4.15) shows that the time-variant term is $(A - L_jC)\breve{X}_k^{ij}$, which means that the differences of $\breve{X}_k^{ij}$ at different time instants, are determined by the shape of $\breve{X}_0^{ij}$, while the contractive factor $A - L_jC$ is determined by the placement of the eigenvalues of $A - L_jC$ (system matrix of the dynamics of the j-th interval observer). Thus, after a waiting time assessed by the eigenvalues of $A - L_jC$ after mode switching, (4.15) enters into its steady state. Then, the set values of $\breve{X}_k^{ij}$ after entering into the steady state can be sufficiently close[1] to the set $\breve{X}_{\infty}^{ij}$, which implies that $\breve{X}_{\infty}^{ij}$ can be used to approximately describe the dynamic behaviors of the whole process after the waiting time. Thus, as long as Theorem 4.1 is satisfied, FDI of all the considered modes can be guaranteed after they occur.

- The considered modes can be detected and isolated at latest when the system enters into steady state, which is implemented by finding the interval observer that estimates residual zonotopes that can include the origin $\mathbf{0}$. Regarding the implementation of FI during the transition, it will be detailed in Section 4.5. □

[1] $\breve{X}_k^{ij}$ is inside the set described as the Minkowski sum of $\{p_{ij}\} \oplus (1+\epsilon)\{\breve{X}_{\infty}^{ij} \oplus \{-p_{ij}\}\}$, where p_{ij} denotes the center of $\breve{X}_{\infty}^{ij}$ and ϵ is a scalar that satisfies $\epsilon > 0$.

Remark 4.10. *According to Section 4.3, at infinity, one has* $R_\infty^{ij} \subseteq \check{R}_\infty^{ij} \subseteq \check{R}_\infty^{ij}$. *Thus, if* $\check{R}_\infty^{ij}$ *satisfies Theorem 4.1, it implies that the same conclusion can be drawn for* R_∞^{ij}, *which guarantees that all the considered modes are detectable and isolable by a bank of interval observers. Similar with Proposition 4.1, if* $R_{k^*}^{ij} \subseteq \check{R}_{k^*}^{ij} \subseteq \check{R}_{k^*}^{ij}$ *holds,* $R_k^{ij} \subseteq \check{R}_k^{ij} \subseteq \check{R}_k^{ij}$ *will always hold for all* $k \geq k^*$. *Since the adaptive bound* $\check{R}_k^{ij}$ *is less conservative than the static bound* $\check{R}_k^{ij}$, *the FI task of this proposed approach is done by using* $\check{R}_k^{ij}$. *This will be detailed in next contents.*

4.4.2 Practical Conditions

Theoretically, $\check{R}_\infty^{ij}$ should be used to establish and check the FDI conditions as explained in Theorem 4.1. However, since $\check{R}_\infty^{ij}$ cannot be accurately computed but only approximated, Theorem 4.1 has only theoretical value.

In order to establish a collection of off-line pre-checkable FDI conditions for practical applications, one has to turn to the approximation of $\check{R}_\infty^{ij}$ defined in Section 4.3. Based on (4.19) and Theorem 4.1, a collection of practical FDI conditions are given as

$$\mathbf{0} \in \mathring{R}_\infty^{ii} \text{ and } \mathbf{0} \notin \mathring{R}_\infty^{ij},\ j \neq i,\ i,\ j \in \mathbb{I}. \tag{4.21}$$

If all the considered modes satisfy (4.21), it is assured that all of them are detectable and isolable by the proposed FDI approach. The FDI conditions are a collection of sufficient but not necessary conditions due to the series of approximations contained in this approach. Thus, their satisfaction can guarantee FDI, but their violation does not imply that the faults are not detectable or isolable with extra efforts.

4.5 Fault Detection and Isolation

Under the satisfaction of the FDI conditions, an FDI algorithm is elaborated in this section to implement actuator FDI.

4.5.1 Fault Detection and Isolation

The proposed approach implements FD by testing whether or not the residual zonotopes estimated by the interval observer matching the current system mode can include the origin at each time instant. The FD principle is summarized in Proposition 4.2.

Proposition 4.2. *If the plant (4.1) is in the steady-state operation of the m-th mode, residual zonotopes estimated by the m-th interval observer can always satisfy*

$$\mathbf{0} \in R_k^{mm},\ m \in \mathbb{I}, \tag{4.22}$$

which implies that, whenever a violation of (4.22) *is detected, it is indicated that a fault has occurred.*

Proof : In the steady-state operation of the m-th mode, the residual zonotopes estimated by the m-th interval observer should always contain the origin as long as there is no mode switching in the system. In other words, if (4.22) is violated, it is guaranteed that the system mode has changed. □

Proposition 4.2 follows the interval observer-based FD approach in [67]. Please refer to Section IV in [67] for the details. In order to explain the FI principle, it is assumed that the system is in the m-th mode and that a fault is detected at time instant k_d. Thus, $R_{k_d}^{fj}$ ($f,\ j \in \mathbb{I} \setminus \{m\}$) can be obtained at time instant k_d, where f denotes the index of a new but unknown mode. Furthermore, for the j-th interval observer, an initial zonotope at time instant k_d, denoted as $\check{X}_{k_d}^{jj}$, which satisfies

$$\check{X}_{k_d}^{jj} \supseteq \tilde{X}_{k_d}^{fj}$$

(i.e., $\check{R}_{k_d}^{jj} \supseteq R_{k_d}^{fj}$) is constructed. This initial zonotope $\check{X}_{k_d}^{jj}$ is used to initialize the dynamics $\check{X}_{k+1}^{jj}$ given by (4.12), which corresponds to the j-th interval observer. After this initialization, one can try to isolate faults during the transition.

Proposition 4.3. *After a fault is detected and the dynamics* (4.12) *of* $\check{X}_{k+1}^{jj}$ *are initialized, if the* j*-th interval observer matches the current and unknown mode,* $\check{R}_k^{jj}$ *should always fully bound* R_k^{fj} *after the FD time instant* k_d*, i.e.,* $\check{R}_k^{jj} \supseteq R_k^{fj}$ *(for all* $k \geq k_d$*), while if the* j*-th interval observer does not match the current mode,* $\check{R}_k^{jj}$ *should only fully contain* R_k^{fj} *at the first several steps after FD and finally diverge.*

Proof : If a mode j appears at time instant k_d (i.e., $f = j$) and $\check{X}_{k_d}^{jj} \supseteq \tilde{X}_{k_d}^{fj}$, it implies $\check{X}_k^{jj} \supseteq \tilde{X}_k^{fj}$ for all $k \geq k_d$ if no other mode switching appears. This implies that $\check{R}_k^{jj} \supseteq R_k^{fj}$ ($k \geq k_d$) should always hold. But if the mode j does not appear, although one assures that $\check{X}_{k_d}^{jj} \supseteq \tilde{X}_{k_d}^{fj}$, because of $f \neq j$, as k tends to infinity, $\mathbf{0} \in \check{R}_k^{jj}$ and $\mathbf{0} \notin R_k^{fj}$ will hold. This can be satisfied under Theorem 4.1 and implies that $\check{R}_k^{jj}$ should only fully contain R_k^{fj} at the first several steps after FD and finally diverge. □

Proposition 4.3 states the transient FI principle proposed in this chapter, which is guaranteed by Theorem 4.1. With respect to each interval observer (excluding the m-th one), the adaptive bound $\check{R}_k^{jj}$ is obtained by initializing the corresponding dynamics of $\check{X}_k^{jj}$. Thus, starting from the FD time k_d, the fault can be isolated by real-time testing whether or not

$$R_k^{fj} \subseteq \check{R}_k^{jj},\ k \geq k_d,\ f,\ j \in \mathbb{I} \setminus \{m\} \tag{4.23}$$

is violated for each interval observer. By testing (4.23) till the time instant when one and only one interval observer can satisfy (4.23), it implies that the current fault is isolated at this time instant and the fault is indexed by the index of the interval observer.

Because of the FDI conditions, one can assure that the fault can be isolated before k reaches infinity. This means that the proposed FI method should be able to isolate the faults at transient state and avoid waiting a period until the complete disappearance of transient behaviors for making FI decisions. But the particular time needed for FI is unknown, which depends on the system dynamics and modes.

Remark 4.11. *For the j-th interval observer, $\check{R}_{k_d}^{jj}$ and $\check{R}_{k_d}^{ij}$ ($i \neq j$, $i,\ j \in \mathbb{I} \setminus \{m\}$) may intersect. If the intersections always contain $R_{k_d}^{fj}$ during the transition, even though the j-th interval observer does not match the new mode, it is still possible that $\check{R}_{k}^{jj} \supseteq R_{k}^{fj}$ ($k \geq k_d$) persistently holds. Consequently, this fact may disturb the FI accuracy of the proposed criterion* (4.23).

In order to solve the problem in Remark 4.11, one turns to the FI mechanism, i.e., testing whether or not

$$\mathbf{0} \in R_k^{fj} \tag{4.24}$$

holds, after the system enters into a new steady state. If (4.24) holds after entering into the steady state of a new mode, it implies that j is the index of the new mode. Otherwise, j does not indicate the new mode and should be removed from the candidate modes. To judge if the system has entered into the steady state of a new mode, it is necessary to define a waiting time. The waiting time is used to describe the duration of the transient behaviors after a fault is detected (see [67] for more details).

Definition 4.1. *The waiting time T is defined as, at least, the maximum of the settling time of all interval observers, such that after a fault is detected, residual zonotopes estimated by the interval observer matching the current system mode include the origin* $\mathbf{0}$ *while residual zonotopes estimated by interval observers not matching the current system mode exclude* $\mathbf{0}$ *after the waiting time.*

Assumption 4.5. *The occurrence of any considered actuator mode is persistent and the persistent time is not shorter than the waiting time.*

According to the previous discussions, the ultimate FI algorithm proposed in this chapter is a combination of the two different FI strategies as in (4.23) and (4.24). Under the satisfaction of Theorem 4.1, the following proposition is used to summarize the proposed FI algorithm.

Proposition 4.4. *Once a fault is detected, the FI strategy* (4.23) *is firstly used to isolate the fault during the transition. If after a waiting time, there are still at least two interval observers that satisfy* (4.23)*, then the FI algorithm is switched into the FI strategy* (4.24) *for the final FI decision.*

Eventually, by combining the FD strategy in Proposition 4.2 and the FI strategy in Proposition 4.4, the effectiveness of the proposed FDI approach can be guaranteed by

Algorithm 1 Proposed FDI algorithm

Require: T, $\hat{X}_0$, mode index $i \in \mathbb{I}$;
Ensure: Fault index f;
Initialization: $i = m$, $f = m$ and $\hat{X}_0^{mj} = \hat{X}_0$ $(m,\ j \in \mathbb{I})$;
At time instant k: Switching $\leftarrow$ FALSE, $\mathbf{0} \in R_k^{mm}$ and $\mathbf{0} \notin R_k^{mj},\ j \in \mathbb{I} \setminus \{m\}$;
while Switching $\neq$ TRUE **do**
  $k \leftarrow k + 1$;
  Obtain R_k^{mm};
  if $\mathbf{0} \notin R_k^{mm}$ **then**
    Switching $\leftarrow$ TRUE;
    Construct initial zonotopes $\check{X}_{k_d}^{jj},\ j \in \mathbb{I} \setminus \{m\}$;
    Initialize all the dynamics $\check{X}_k^{jj}$ described by (4.12);
  end if
end while
$\mathbb{I}_m$=$\mathbb{I} \setminus \{m\}$;
Timer = T;
while Timer $\neq$ 0 **do**
  $k \leftarrow k + 1$;
  if length($\mathbb{I}_m$)$\neq$ 1 **then**
    Obtain all R_k^{fj} and $\check{R}_k^{jj}$, $f,\ j \in \mathbb{I}_m$;
    for $j \in \mathbb{I}_m$ **do**
      if $R_k^{fj} \not\subseteq \check{R}_k^{jj}$ **then**
        Remove j from $\mathbb{I}_m$;
      end if
    end for
  end if
  if length($\mathbb{I}_m$)= 1 **then**
    $f = \mathbb{I}_m$;
    Timer=0
  else
    Timer = Timer - 1;
  end if
end while
if $f = m$ **then**
  Obtain all $R_k^{fj},\ j \in \mathbb{I}_m$;
  for $j \in \mathbb{I}_m$ **do**
    if $\mathbf{0} \notin R_k^{fj}$ **then**
      Remove j from $\mathbb{I}_m$;
    end if
  end for
  $f = \mathbb{I}_m$;
end if
return f;

Theorem 4.1. The FDI procedure of the proposed approach is summarized in Algorithm 1, where length(·) computes the number of the elements of a set. Finally, there will be one and only one element in $\mathbb{I}_m$ that indicates the new mode, for simplicity, the notation $f = \mathbb{I}_m$ is directly used at the end of the algorithm.

4.5.2 Initial Zonotopes

It is assumed that a fault is detected at time instant k_d. As per Section 4.5.1, at the FD time k_d, all the corresponding bounding zonotope dynamics $\check{X}_k^{jj}$ ($j \in \mathbb{I} \setminus \{m\}$) should be initialized by their corresponding initial zonotopes, denoted as $\check{X}_{k_d}^{jj}$, such that

$$\check{X}_{k_d}^{jj} \supseteq \tilde{X}_{k_d}^{fj}, \tag{4.25}$$

implying that $\check{R}_{k_d}^{jj} \supseteq R_{k_d}^{fj}$ ($f,\ j \in \mathbb{I} \setminus \{m\}$) holds. This initialization is a key for the proposed approach to implement FDI during the transition. Thus, a key point is to construct $\check{X}_{k_d}^{jj}$ for all the corresponding dynamics of $\check{X}_k^{jj}$.

The idea is to use the obtainable information $R_{k_d}^{fj}$ at time instant k_d to construct the zonotope $\check{X}_{k_d}^{jj}$ satisfying (4.25). By defining a zonotope $V_0 = H_{\bar{\eta}}\mathbb{B}^q$, (4.10) can be transformed into

$$R_k^{fj} = C\tilde{X}_k^{fj} \oplus \{\eta_k - \eta^c\} \oplus (-V_0). \tag{4.26}$$

By adding $-(\eta_k - \eta^c)$ to both sides of (4.26), the equation (4.26) turns into

$$R_k^{fj} \oplus \{-(\eta_k - \eta^c)\} = C\tilde{X}_k^{fj} \oplus (-V_0). \tag{4.27}$$

Considering $-(\eta_k - \eta^c) \in (-V_0)$, one can further obtain

$$C\tilde{X}_k^{fj} \oplus (-V_0) \subseteq R_k^{fj} \oplus (-V_0). \tag{4.28}$$

Eventually, a key expression is obtained from (4.28) as

$$C\tilde{X}_k^{fj} \subseteq R_k^{fj}. \tag{4.29}$$

Since R_k^{fj} is a zonotope, it can be written in the zonotopic form

$$R_k^{fj} = r_k^{fj,c} \oplus H_k^{fj,r}\mathbb{B}^{s_k^{fj,r}}.$$

By using the zonotopic form of R_k^{fj}, (4.29) can be equivalently expressed as a group of q inequalities and the l-th inequality out of the q inequalities has the form

$$|\ C(l)\tilde{x}_k^{fj} - r_k^{fj,c}(l)\ | \leq \|\ H_k^{fj,r}(l)\ \|_1, \quad l = 1, 2, \ldots, q, \tag{4.30}$$

where $C(l)$ denotes the l-th row of C, and $r_k^{fj,c}(l)$ and $H_k^{fj,r}(l)$ denote the l-th component of $r_k^{fj,c}$ and the l-th row of $H_k^{fj,r}$.

According to Property 2.4 in Chapter 2, each inequality out of the q inequalities of (4.30) determines a strip. This implies that the q strips determined by the q inequalities should form a closed set. This closed set (denoted as $\bar{X}_k^{fj}$) can be computed by using Property 2.4. Note that $\bar{X}_k^{fj}$ is able to contain $\tilde{X}_k^{fj}$ (i.e., $\bar{X}_k^{fj} \supseteq \tilde{X}_k^{fj}$), which can be used as an initial zonotope that satisfies (4.25) at time instant k_d, i.e.,

$$\check{X}_{k_d}^{jj} = \bar{X}_{k_d}^{fj}.$$

However, since Property 2.4 can only compute a zonotope approximation for the intersection of a zonotope and a strip, in order to construct $\bar{X}_k^{fj}$, an initial zonotope has to be given to the approach proposed in Property 2.4 as a starting set.

Remark 4.12. *The initial zonotope (denoted as $\tilde{X}$) for the method given in Property 2.4 is defined as a zonotope that contains the physical constraint set of $\tilde{X}_k^{fj}$ for any interval observer in any mode. Since there always exist the physical constraints on any system, a proper set $\tilde{X}$ can be easily found.*

Thus, by using $\tilde{X}$ as an initial zonotope for Property 2.4, at the FD time instant k_d, $\bar{X}_{k_d}^{fj}$ can be computed as the initial zonotope $\check{X}_{k_d}^{jj}$ to initialize the dynamics of the corresponding bounding zonotopes $\check{X}_k^{jj}$ ($j \in \mathbb{I}\backslash\{m\}$) described by (4.12). Using the generated residual-bounding zonotope sequences, FDI during the transition can be implemented. Note that, in the case that C is invertible, (4.29) can be transformed into

$$\tilde{X}_k^{fj} \subseteq C^{-1} R_k^{fj},$$

where C^{-1} represents the inverse of C. In this case, at the FD time k_d, $C^{-1}R_{k_d}^{fj}$ is directly used as the initial zonotope $\check{X}_{k_d}^{jj}$.

Remark 4.13. *In order to construct the initial zonotope at the FD time k_d, a method is proposed by using Property 2.4. However, one can still introduce another method based on Property 2.5 to construct the initial zonotope, where Property 2.5 computes a zonotopic approximation of the intersection between a polytope and a zonotope. Using Property 2.5, one can use all the q strips (5.32) as a whole (i.e., a polytope) and compute the zonotopic approximation of the intersection of this polytope and a zonotope $\tilde{X}$ in Remark 4.12 to construct the initial zonotope. For particular applications, the designer can choose one out of the two methods to construct the initial zonotope.*

4.6 Illustrative Example

In this chapter, a CSTR from [38] is used to illustrate the effectiveness of this approach. The CSTR considers an exothermic irreversible reaction $A \rightarrow B$. Based on the reactant

mass balance and energy balance in the reactor, the process is depicted by a non-linear dynamic model given in [38] (please read [38] for all the details about the CSTR case study in this chapter). As per [38], c_A is the concentration of the component A, T is the reactor temperature, q_c is the input and c_A is the output, and the nominal values for the CSTR model parameters are given in Table 4.1. The operating point of the CSTR is chosen as

$$c_{A_o} = 8.235 \times 10^{-2} \text{mol/l}, \tag{4.31a}$$
$$T_o = 441.81 \text{K}. \tag{4.31b}$$

The discrete-time linear model of the system around the operating point defined by (4.31) is obtained as

$$x_{k+1} = \begin{bmatrix} 0.8976 & -0.0002 \\ -0.4894 & 0.7606 \end{bmatrix} x_k + \begin{bmatrix} 0 \\ 0.0024 \end{bmatrix} F u_k + \omega_k^i, \tag{4.32a}$$
$$y_k = \begin{bmatrix} 1 & 0 \end{bmatrix} x_k, \tag{4.32b}$$

where ω_k^i is a bounded signal to model the discretization errors[1] between the linearized continuous-time model and linear discrete-time model for the i-th mode. The proposed approach only requires the bounds of ω_k^i and does not require their real-time values. In simulation, empirical values are given for the bounds of ω_k^i, which are obtained as

$$\bar{\omega}^0 = \begin{bmatrix} 0.001 & 0.001 \end{bmatrix}^T, \omega^{0_c} = \begin{bmatrix} 0 & 0 \end{bmatrix}^T, \tag{4.33a}$$
$$\bar{\omega}^1 = \begin{bmatrix} 0.002 & 0.002 \end{bmatrix}^T, \omega^{1_c} = \begin{bmatrix} 0.015 & 0.015 \end{bmatrix}^T, \tag{4.33b}$$
$$\bar{\omega}^2 = \begin{bmatrix} 0.003 & 0.003 \end{bmatrix}^T, \omega^{2_c} = \begin{bmatrix} 0.03 & 0.03 \end{bmatrix}^T. \tag{4.33c}$$

Remark 4.14. *Since the proposed FDI approach considers the linear discrete time-invariant systems, while the CSTR is a highly non-linear system, in this case study, the simulations are done based on the linearized model of the CSTR and ω_k^i is empirically decided by simulations.*

Faults affecting the valve position corresponding to the coolant flow are considered, i.e., the flow rate of the coolant is affected. Thus, the faults are modelled as F in (4.32), where 0 and 1 denote the complete outage and healthy operation of the valve, respectively, and a value inside $(0, 1)$ denotes that the valve loses partial performance. Here, two faults are considered, i.e., F_0 (healthy), F_1 (fault 1) and F_2 (fault 2). It is known the particular magnitude of faults is unknown in reality. Thus, one considers the bounds of F_1 and F_2, which are denoted as intervals

$$\mathbf{F}_1 = [0.1, 0.3], \ \mathbf{F}_2 = [0.5, 0.7]. \tag{4.34}$$

[1] Realistically, the errors are possible to be different for different modes, which does not conflict with (4.1).

If $\mathbf{F}_1$ and $\mathbf{F}_2$ satisfy the proposed FDI conditions, a fault occurrence with any fault magnitude inside $\mathbf{F}_1$ or $\mathbf{F}_2$ is detectable and isolable. These two operating regions $\mathbf{F}_1$ and $\mathbf{F}_2$ of the valve are monitored by two interval observers. Whenever the operating situation of the valve drops into either of the two regions, they can be detected and isolated by the proposed approach.

Based on (4.32) and (4.34), three interval observers with the form indicated in (4.4) and (4.5) are designed to monitor the linearized continuous-time model. The gain matrices and initial conditions for the interval observers and the waiting time for the steady-state FI are given as:

- Observer gains: $L_0 = L_1 = L_2 = \begin{bmatrix} 0.1582 \\ 11.6106 \end{bmatrix}$.
- Initial conditions: $x_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $\hat{X}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 0.05 & 0 & 0.05 \\ 0.05 & 0.05 & 0 \end{bmatrix} \mathbb{B}^3$.
- Waiting time T: $T = 20\Delta t$.

The actual magnitudes of actuator faults are given as

$$F_1 = 0.15,\ F_2 = 0.55,$$

which are inside the bounds indicated in (4.34), respectively. In simulation, the input around the operating point is a sinusoidal signal that oscillates in an interval

$$\Delta q_c \in [-20, 20].$$

According to Theorem 2.1 and Proposition 2.1 and iterating (4.15) thirty steps, as explained in Section 4.3.3, the RPI approximations of the limit sets of the static residual-bounding zonotpes for each interval observer are computed. Furthermore, the interval hulls of these RPI approximations are presented as:

- For interval observer 0:

$$\mathring{R}_\infty^{10} = [0.0477,\ 0.0719],$$
$$\mathring{R}_\infty^{20} = [0.1035,\ 0.1356].$$

- For interval observer 1:

$$\mathring{R}_\infty^{01} = [-0.0719,\ -0.0477],$$
$$\mathring{R}_\infty^{21} = [0.0396,\ 0.0799].$$

Table 4.1: Parameters of CSTR

Variable	Symbol	Nominal value
Tank volume	V	100 [l]
Feed flow rate	q	100 [l/min]
Feed concentration	c_{Af}	1 [mol/l]
Feed temperature	T_f	350 [K]
Coolant flow rate	q_c	100 [mol/l]
Coolant temperature	T_c	350 [K]
Densities	ρ, ρ_c	1000 [g/l]
Specific heats	C_p, C_{pc}	1 [cal/(g K)]
Pre-exponential factor	k_0	7.2×10^{10} [1/min]
Exponential factor	E/R	9.98×10^3 [K]
Heat of reaction	$-\Delta H$	2.0×10^5 [cal/mol]
Heat transfer charact.	hA	7.0×10^5 [1/(min K)]
Sampling period	Δt	0.1 [min]

- For interval observer 2:

$$\mathring{R}_{\infty}^{02} = [-0.1356,\ -0.1035],$$
$$\mathring{R}_{\infty}^{12} = [-0.0799,\ -0.0396].$$

As per the discussions in this chapter, $\mathring{R}_{\infty}^{00}$, $\mathring{R}_{\infty}^{11}$ and $\mathring{R}_{\infty}^{22}$ can always include $\mathbf{0}$, they are omitted here. It can be observed that all the RPI approximations corresponding to a bank of interval observers satisfy the FDI conditions as established in (4.19), which implies that the proposed technique can be used for FDI.

Remark 4.12 suggests an initial zonotope $\tilde{X}$ determined by the plant physical constraints. $\tilde{X}$ is used by Property 2.4 to construct initial zonotopes for the initialization of the dynamics of the static residual-bounding zonotopes whenever a fault is detected. By simulations, $\tilde{X}$ is empirically given as

$$\tilde{X} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 0.15 & 0 & 0.15 \\ 0 & 5 & 5 \end{bmatrix} \mathbb{B}^3,$$

which can bound $\tilde{X}_k^{ij}$ in any mode. Besides, the parameter λ in Property 2.4 (note that a selection strategy of λ can be found in [2]) is given as

$$\lambda = \begin{bmatrix} 1 & 1 \end{bmatrix}^T.$$

In this example, the fault modes 1 and 2 are simulated separately. The fault scenarios for both fault modes are set as follows: from time instants 0 to 49, the actuator

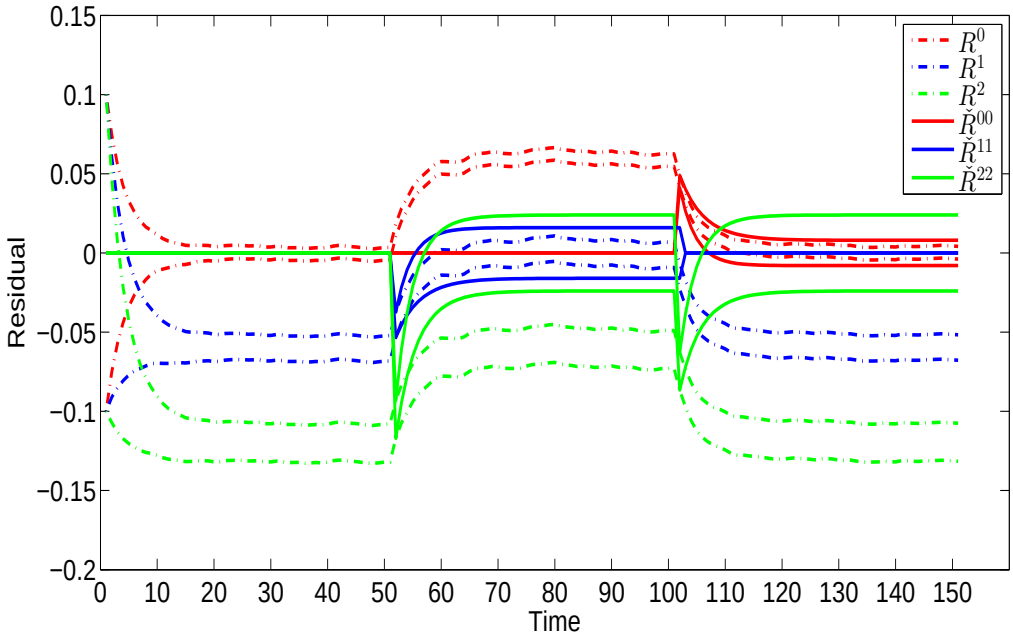


Figure 4.2: FDI of Fault 1

is healthy, from time instants 50 to 99 an actuator fault occurs and from time instants 100 to 150 the actuator recovers to the healthy mode.

The simulation results of the fault 1 are presented in Figure 4.2. From time instants 0 to 49, the actuator is healthy, thus, residual zonotopes[1] (R^0 in Figure 4.2) estimated by the healthy interval observer can always contain the origin. At time instant 50, the fault 1 occurs. Then, R^0 excludes the origin at time instant 52, which indicates that the fault is detected at time instant 52.

At the same time, $\check{R}^{11}$ and $\check{R}^{22}$ corresponding to the interval observers 1 and 2 are initialized to start the transient FI task. At time instant 53, it can be observed that $R^1 \subseteq \check{R}^{11}$ but $R^2 \nsubseteq \check{R}^{22}$, which implies that the fault 2 does not occur while the fault 1 has occurred in the system. The same conclusion can be drawn when one analyzes the steady-state behaviors and it can be observed that $\mathbf{0} \in R^1$, $\mathbf{0} \notin R^0$ and $\mathbf{0} \notin R^2$ after T, which also indicates that the fault 1 has occurred in the system. Besides, from time instants 100 to 150, a recovery process is introduced, which can be understood in the same way. Regarding the fault 2, the results are given in Figure 4.3, which can be explained similarly as the fault 1. Thus, as per the results, the proposed FDI technique is

[1]For theoretical analysis, one uses R_k^{ij} to denote the residual zonotope estimated by the j-th interval observer in the i-th mode at time instant k. But, in the figures, one only uses R^i to denote the residual zonotopes from the i-th interval observer.

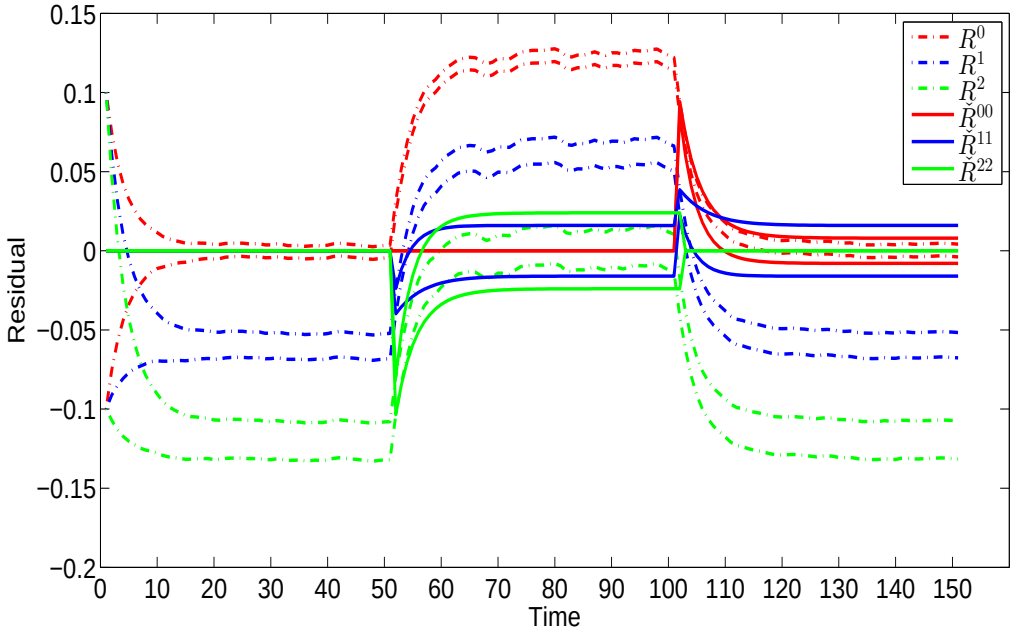


Figure 4.3: FDI of Fault 2

effective to detect the faults and further isolate the faults during the transition between two different modes.

Remark 4.15. *There are two different FI strategies in the proposed FDI approach. One is for the transient-state FI and the other is for the steady-state FI. However, notice that the emphasis of the proposed FI approach consists in the transient-state FI strategy, while the steady-state FI strategy is used as FI guarantees of the transient-state FI strategy when the transient-state FI strategy loses its effectiveness.*

4.7 Summary

In this chapter, an actuator FDI approach using a bank of interval observers is proposed, where invariant set-based FDI conditions are established to guarantee FDI. Under the FDI conditions, the approach can provide two different FI mechanisms that can be selected according to the need of actual applications. The first FI mechanism can isolate faults during the transition between induced by mode switching while the second one usually needs more time to isolate faults but with less computational load. The future research consists in loosening the FDI conditions and extending the approach into the system with parametric uncertainties.

Chapter 5

Sensor-fault Detection and Isolation using Set-based Methods

In this chapter, the main objective is to propose a sensor FDI approach based on interval observers. For the set-based approach, the important challenge is how to reduce the conservatism of guaranteed FDI conditions as much as possible. In this chapter, based on invariant sets, a collection of guaranteed FDI conditions are established by using the system-operating information from all interval observers. If all considered sensor faults satisfy the FDI conditions, it can be guaranteed that they are detectable and isolable. This chapter concludes with a case study based on a subsystem of a wind turbine benchmark, which illustrates the effectiveness of the proposed technique.

5.1 Introduction

In [65–67], interval observers have been extended for FDI in terms of actuator faults. However, considering differences between actuator and sensor faults, if one applies the approach proposed in Chapter 4 into sensor FDI, the obtained results will be more conservative in terms of FDI guarantees. In order to obtain a less conservative set-based sensor FDI approach, one proposes a method to make full use of all available and useful system-operating information and simultaneously reduce computational complexity as much as possible.

This chapter aims to propose a set-based robust sensor FDI approach with no need of multisensor redundancy [58]. It has been stated that, to improve the set-based FDI approach, one has to propose tighter guaranteed FDI conditions. Additionally, because of different characteristics of actuator and sensor faults, comparing with the works for actuator FDI [65, 66], the approach proposed in this chapter pays more extra efforts to implement set-based robust detection and isolation for sensor faults.

The contribution of the approach proposed in this chapter is threefold. First, the FDI decision is jointly made by both interval observer-based and the invariant set-based FDI mechanisms. Second, the proposed approach uses the system-operating information captured by all interval observers for establishing FDI conditions and implementing FDI. Third, in this FDI approach, a mechanism to reduce computational complexity as much as possible is also proposed, which aims to obtain a balance between FDI performance and computational complexity.

5.2 Problem Formulation

5.2.1 Plant Models

The proposed sensor FDI scheme has the same structure as that in Figure 4.1, where the linear discrete time-invariant plant under the effect of sensor faults is modelled as

$$x_{k+1} = Ax_k + Bu_k + \omega_k, \tag{5.1a}$$
$$y_k = G_i C x_k + \eta_k. \tag{5.1b}$$

In the model (5.1), G_i ($i \in \mathbb{I} = \{0, 1, \cdots, M\}$) is a $q \times q$ diagonal matrix[1] used to model the i-th sensor mode, where M denotes the number of the considered sensor faults. Besides, G_0 is the identity matrix denoting the healthy sensor mode, while G_i ($i \neq 0$) denotes the i-th sensor-fault mode, whose diagonal elements take values[2] from an interval $[0, 1]$.

Remark 5.1. *The number M of the considered sensor faults is different from that of sensors in a system, because there may be several fault modes critical to the system performance/safety corresponding to one sensor, which should be monitored on-line. Thus, in this approach, $M + 1$ interval observers are designed, each of which corresponds to one sensor mode.*

Assumption 5.1. *The pair (A, B) is stabilizable and the pairs $(A, G_i C)$ are detectable for all $i \in \mathbb{I}$.*

Assumption 5.2. *The occurrence of any considered mode can persist sufficiently long time such that the FDI module has enough responsive time to detect and isolate them.*

Since the scheme in Figure 4.1 is open-loop, which does not take the effect of inputs on the system stability into account. Realistically, one should firstly assure system stability for analyzing the proposed approach.

[1] Each row of C corresponds to a sensor and the status of the i-th sensor is modelled by the value of the i-th diagonal element of G_i.

[2] For the diagonal elements of G_i, taking the values 0 and 1 denotes the complete outage and health of the corresponding sensor, respectively, while taking a value inside the interval $(0, 1)$ denotes partial performance degradation of the corresponding sensor.

The proposed approach can be used for both single or multiple faults. For single faults, the fault-modelling matrix G_i for each considered mode only has one diagonal element not equal to 1, while for multiple faults, G_i has several different diagonal elements not equal to 1. More details will be presented in this chapter.

5.2.2 Interval Observers

In Figure 4.1, a bank of interval observers are used to monitor the considered modes. In accordance with the model (5.1), the interval observer corresponding to the j-th ($j \in \mathbb{I}$) mode is designed as

$$\hat{X}_{k+1}^{j} = (A - L_j G_j C)\hat{X}_k^j \oplus \{Bu_k\} \oplus \{L_j y_k\} \oplus (-L_j)V \oplus W, \tag{5.2a}$$

$$\hat{Y}_k^j = G_j C \hat{X}_k^j \oplus V, \tag{5.2b}$$

where $\hat{X}_k^j$ and $\hat{Y}_k^j$ are the state and output sets estimated by the j-th interval observer, respectively, and the gain L_j is chosen to guarantee that $A - L_j G_j C$ is a Schur matrix.

Assumption 5.3. *The initial state of the plant and the initial state set of all interval observers are denoted as x_0 and $\hat{X}_0$, respectively, and $x_0 \in \hat{X}_0$ holds.*

Remark 5.2. *For each interval observer, its initial set can be different. However, for simplicity, a common set is used as the initial set for all interval observers.*

Since W and V are zonotopes, if the initial set $\hat{X}_0$ is chosen as a zonotope, $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ are also zonotopes. By using zonotope operations, (5.2) can be transformed into the equivalent center-segment matrix form

$$\hat{x}_{k+1}^{j,c} = (A - L_j G_j C)\hat{x}_k^{j,c} + Bu_k + L_j y_k - L_j \eta^c + w^c, \tag{5.3a}$$

$$\hat{H}_{k+1}^{j,x} = [(A - L_j G_j C)\hat{H}_k^{j,x} \quad -L_j H_{\bar{\eta}} \quad H_{\bar{\omega}}], \tag{5.3b}$$

$$\hat{y}_k^{j,c} = G_j C \hat{x}_k^{j,c} + \eta^c, \tag{5.3c}$$

$$\hat{H}_k^{j,y} = [G_j C \hat{H}_k^{j,x} \quad H_{\bar{\eta}}], \tag{5.3d}$$

where $\hat{x}_k^{j,c}$, $\hat{y}_k^{j,c}$, $\hat{H}_k^{j,x}$ and $\hat{H}_k^{j,y}$ are the centers and segment matrices of $\hat{X}_k^j$ and $\hat{Y}_k^j$, respectively.

Remark 5.3. *Under Assumptions 5.1 and 5.3, the state x_k should be always contained inside the state set estimated by the interval observer matching the current system mode at steady state if there is no mode switching. The same results hold for the output and corresponding estimated output set.*

5.3 Residual Analysis

In this section, for the proposed FDI technique, residuals are defined in terms of zonotopes and the corresponding bounding sets of residual zonotopes are derived.

5.3.1 Residual Zonotopes

If the system currently operates in the i-th mode, the residual zonotope corresponding to the j-th interval observer at time instant k is defined as

$$\begin{aligned} R_k^{ij} =& \{y_k\} \oplus (-\hat{Y}_k^j) \\ =& \{G_i C x_k + \eta_k\} \oplus (-G_j C \hat{X}_k^j) \oplus (-V) \\ =& G_j C\{\{x_k\} \oplus (-\hat{X}_k^j)\} \oplus \{(G_i - G_j) C x_k\} \oplus \{\eta_k\} \oplus (-V), \end{aligned} \tag{5.4}$$

where, denoting by $\tilde{X}_k^{ij}$ the term $\{x_k\} \oplus (-\hat{X}_k^j)$, the residual zonotope is rewritten as

$$R_k^{ij} = G_j C \tilde{X}_k^{ij} \oplus \{(G_i - G_j) C x_k\} \oplus \{\eta_k\} \oplus (-V). \tag{5.5}$$

Moreover, since $\tilde{X}_{k+1}^{ij}$ is a zonotope, $\tilde{x}_{k+1}^{ij,c}$ and $\tilde{H}_{k+1}^{ij,x}$ are used to denote its center and segment matrix, respectively. Thus, by using (5.1) and (5.3), one can have

$$\tilde{x}_{k+1}^{ij,c} = x_{k+1} - \hat{x}_{k+1}^{j,c}, \tag{5.6a}$$

$$\tilde{H}_{k+1}^{ij,x} = \hat{H}_{k+1}^{j,x}, \tag{5.6b}$$

where, using (5.1), (5.3) and (5.6), $\tilde{x}_{k+1}^{ij,c}$ and $\tilde{H}_{k+1}^{ij,x}$ can be further derived as

$$\tilde{x}_{k+1}^{ij,c} = (A - L_j G_j C)\tilde{x}_k^{ij,c} + L_j(G_j - G_i) C x_k - L_j(\eta_k - \eta^c) + \omega_k - \omega^c, \tag{5.7a}$$

$$\tilde{H}_{k+1}^{ij,x} = \hat{H}_{k+1}^{j,x} = [(A - L_j G_j C)\hat{H}_k^{j,x} \quad - L_j H_{\bar{\eta}} \quad H_{\bar{\omega}}]. \tag{5.7b}$$

5.3.2 Residual-bounding Zonotopes

In (5.7), one cannot measure $\tilde{x}_k^{ij,c}$ since it involves unmeasurable quantities (η_k, ω_k and x_k). Thus, to precisely describe the bounds of residual zonotopes, one needs to consider residual-bounding zonotopes which are defined to contain the corresponding residual zonotopes. In order to obtain residual-bounding zonotopes, Assumption 4.4 is made for the plant inputs. For construction of invariant sets, the system dynamics (5.1a) can be rewritten as

$$x_{k+1} = A x_k + [B \;\; I] \begin{bmatrix} u_k \\ \omega_k \end{bmatrix}. \tag{5.8}$$

Considering $u_k \in U$ and $\omega_k \in W$ as in Assumption 4.4 and (3.2), an RPI set, denoted as X, can be constructed to confine the states of the dynamics (5.8) by using Theorem 2.1 and Proposition 2.1.

Remark 5.4. *Any set $X \subset \mathbb{R}^n$ invariant with respect to the dynamics (5.8) is also invariant with respect to all modes (healthy or faulty). This statement holds since the dynamics (5.8) are not affected by these sensor faults directly or indirectly, as long as the inputs are bounded by the same set.*

Since U and W are considered as zonotopes, X is also a zonotope and is denoted as

$$X = x^c \oplus H_x \mathbb{B}^n,$$

where x^c and H_x are the center and segment matrix, respectively. By substituting X, W and V into (5.7) to replace x_k, ω_k and η_k, respectively, a bounding zonotope (denoted as $\check{X}_{k+1}^{ij}$ with the center $\check{x}_{k+1}^{ij,c}$ and segment matrix $\check{H}_{k+1}^{ij,x}$) to contain $\tilde{X}_{k+1}^{ij}$ is obtained as

$$\check{x}_{k+1}^{ij,c} = (A - L_j G_j C)\check{x}_k^{ij,c} + L_j(G_j - G_i)Cx^c, \tag{5.9a}$$

$$\check{H}_{k+1}^{ij,x} = [(A - L_j G_j C)\check{H}_k^{j,x} \;\; L_j(G_j - G_i)CH_x \;\; -L_j H_{\bar{\eta}} \;\; H_{\bar{\omega}} \;\; L_j H_{\bar{\eta}} \;\; -H_{\bar{\omega}}]. \tag{5.9b}$$

Note that, comparing (5.7) with (5.9), it can be observed that (5.9) is the set-valued version of (5.7) by considering the bounds of states and uncertainties.

Remark 5.5. *As per* (5.7) *and* (5.9)*, if* $\tilde{X}_{k^*}^{ij} \subseteq \check{X}_{k^*}^{ij}$ *holds,* $\tilde{X}_k^{ij}$ *should always be contained by* $\check{X}_k^{ij}$ *for all* $k \geq k^*$.

Furthermore, as per (5.5) and Remark 5.5, one obtains a residual-bounding zonotope $\check{R}_k^{ij}$ to contain R_k^{ij}:

$$\check{R}_k^{ij} = G_j C \check{X}_k^{ij} \oplus (G_i - G_j)CX \oplus V \oplus (-V). \tag{5.10}$$

For the center-segment matrix description, an equivalent set description[1] of (5.9) is obtained as

$$\check{X}_{k+1}^{ij} = (A - L_j G_j C)\check{X}_k^{ij} \oplus L_j(G_j - G_i)CX \oplus L_j V \oplus (-W) \oplus (-L_j V) \oplus W. \tag{5.11}$$

As stated in Proposition 2.1, as k tends to infinity, the set sequence generated by (5.11) converges to the mRPI set of the dynamics (5.7) if one considers $x_k \in X$, $\omega_k \in W$ and $\eta_k \in V$, and an RPI approximation of the mRPI set with an arbitrarily expected precision can be constructed by iterating (5.11) from an initial RPI set of (5.7).

5.4 Fault Detection and Isolation Conditions

This section proposes a novel set-based FDI strategy for sensor faults by combining both interval observer-based and invariant set-based FDI mechanisms.

5.4.1 Collecting Process Information

At each time instant, the system operation can be monitored in terms of residual zonotopes by means of a bank of interval observers. For brevity, in the i-th mode, one defines a vector[2] of residual zonotopes to collect residual zonotopes estimated by all

[1] The equivalence of (5.9) and (5.11) can be verified by applying zonotope operations into (5.11) to obtain its center-segment matrix equivalent form, which is the same with (5.9).

[2] Because, in any mode, residual zonotopes are obtainable, without ambiguity, the notation $\mathbf{R}_k^i$ corresponding to the i-th mode can be generally replaced by the notation $\mathbf{R}_k$.

interval observers at time instant k, i.e.,

$$\mathbf{R}_k^i = (R_k^{i0}, R_k^{i1}, \cdots, R_k^{iM}). \tag{5.12}$$

Table 5.1: Residual zonotopes

	Interval Observer 0	$\cdots$	Interval Observer i	$\cdots$	Interval Observer M
Mode 0	R_k^{00}	$\cdots$	R_k^{0i}	$\cdots$	R_k^{0M}
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode i	R_k^{i0}	$\cdots$	R_k^{ii}	$\cdots$	R_k^{iM}
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode M	R_k^{M0}	$\cdots$	R_k^{Mi}	$\cdots$	R_k^{MM}

Remark 5.6. *In this chapter, the indices of rows and columns of tables and matrices start from* 0*. The index* 0 *corresponds to the healthy mode and interval observer.*

Table 5.2: Limit sets of residual-bounding zonotopes

	Interval Observer 0	$\cdots$	Interval Observer i	$\cdots$	Interval Observer M
Mode 0	$\check{R}_\infty^{00}$	$\cdots$	$\check{R}_\infty^{0i}$	$\cdots$	$\check{R}_\infty^{0M}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode i	$\check{R}_\infty^{i0}$	$\cdots$	$\check{R}_\infty^{ii}$	$\cdots$	$\check{R}_\infty^{iM}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode M	$\check{R}_\infty^{M0}$	$\cdots$	$\check{R}_\infty^{Mi}$	$\cdots$	$\check{R}_\infty^{MM}$

Furthermore, if considering residual zonotopes corresponding to all the considered modes and interval observers, one can collect all available real-time system-operating information, which is presented in Table 5.1. Except the real-time process-operating information conveyed by residual zonotopes estimated by a bank of interval observers, there exist additional off-line process information provided by the limit sets of all the corresponding residual-bounding zonotopes. Table 5.2 collects the limit sets of all residual-bounding zonotopes, i.e., the smallest sets of residual zonotopes. Each row of Table 5.2 corresponds to a sensor mode. Thus, from Table 5.2, a matrix describing all the considered modes can be extracted as

$$\mathbf{M} = \begin{bmatrix} \check{R}_\infty^{00} & \cdots & \check{R}_\infty^{0i} & \cdots & \check{R}_\infty^{0M} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \check{R}_\infty^{i0} & \cdots & \check{R}_\infty^{ii} & \cdots & \check{R}_\infty^{iM} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \check{R}_\infty^{M0} & \cdots & \check{R}_\infty^{Mi} & \cdots & \check{R}_\infty^{MM} \end{bmatrix}. \tag{5.13}$$

Remark 5.7. *Comparing Table 5.1 with 5.2, it is known that, in the steady-state operation, the element in each entry of Table 5.2 is the set of that in the corresponding entry of Table 5.1 such as* $R_k^{i0} \subseteq \breve{R}_\infty^{i0}$ *when* k *is sufficiently large. Similarly, one has* $\mathbf{R}_k^i \subseteq \mathbf{M}^i$, *(*$i \in \mathbb{I}$*), where* $\mathbf{M}^i$ *is the* i*-th row of* $\mathbf{M}$ *and* $\subseteq$ *should be understood elementwise.*

Table 5.3: Transformation of Table 5.2

	Interval Observer 0	$\cdots$	Interval Observer i	$\cdots$	Interval Observer M
Mode 0	1	$\cdots$	$1\backslash 0$	$\cdots$	$1\backslash 0$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode i	$1\backslash 0$	$\cdots$	1	$\cdots$	$1\backslash 0$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode M	$1\backslash 0$	$\cdots$	$1\backslash 0$	$\cdots$	1

In order to simplify Table 5.2, one defines the following rules: first, if $\mathbf{0} \in \breve{R}_\infty^{ij}$, the position of $\breve{R}_\infty^{ij}$ is labelled as 1. Second, if $\mathbf{0} \notin \breve{R}_\infty^{ij}$, the position of $\breve{R}_\infty^{ij}$ is labelled as 0. After applying the rules for Table 5.2, Table 5.3 is generated, containing binary information in concordance with the above logical propositions. Notice that, as per the interval observer-based FDI principle, $\mathbf{0} \in R_k^{ii} \subseteq \breve{R}_\infty^{ii}$ should always hold in the steady-state operation of the i-th mode for all $i \in \mathbb{I}$. Similarly, from Table 5.3, a matrix describing all the collected off-line mode information can be obtained as

$$\mathcal{I} = \begin{bmatrix} 1 & \cdots & 1\backslash 0 & \cdots & 1\backslash 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1\backslash 0 & \cdots & 1 & \cdots & 1\backslash 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1\backslash 0 & \cdots & 1\backslash 0 & \cdots & 1 \end{bmatrix}. \tag{5.14}$$

5.4.2 Fault Detection and Isolation Conditions

After collecting all available information as in the matrix (5.14), one should analyze how much information is useful and how much is available but redundant/unnecessary for FDI. It is mentioned that all the diagonal entries of the matrix (5.14) are 1 because $\mathbf{0} \in R_k^{ii}$ and $R_k^{ii} \subseteq \breve{R}_k^{ii}$ always holds in the steady-state operation of the i-th mode. For the non-diagonal entries of the matrix (5.14), one does not know theoretically whether or not they are $\mathbf{0}$ in advance. In this case, one should consider two possibilities:

- For the non-diagonal entries with 0, one has $\mathbf{0} \notin R_\infty^{ij}$ $(i \neq j)$, because $R_\infty^{ij} \subseteq \breve{R}_\infty^{ij}$ and $\mathbf{0} \notin \breve{R}_\infty^{ij}$ imply $\mathbf{0} \notin R_\infty^{ij}$.
- For the non-diagonal entries with 1, one does not have $\mathbf{0} \in R_\infty^{ij}$ $(i \neq j)$, because $R_\infty^{ij} \subseteq \breve{R}_\infty^{ij}$ and $\mathbf{0} \in \breve{R}_\infty^{ij}$ do not guarantee $\mathbf{0} \in R_\infty^{ij}$.

Since the non-diagonal entries with 1 in the matrix $\mathcal{I}$ cannot guarantee that their corresponding residual zonotopes at infinity in Table 5.1 contain $\mathbf{0}$, these entries are not useful for the proposed FDI approach and the residual-bounding zonotopes corresponding to these entries should be discarded in order to reduce computational complexity. Comparatively, the non-diagonal entries with 0 can guarantee that the residual zonotopes corresponding to them do not contain $\mathbf{0}$ at infinity, which are useful for the proposed FDI approach. More details can be presented in next sections.

In this chapter, the proposed FDI approach is based on the combined use of residual zonotopes and residual-bounding zonotopes. Residual zonotopes estimated by interval observers can always be obtained in real time. Residual-bounding zonotopes are generated especially for the transient-state FI after a fault is detected. The limit sets of residual-bounding zonotopes (in Table 5.2) are mainly used for establishing guaranteed FDI conditions, which are used for off-line pre-checking in advance whether or not the considered modes are detectable and isolable.

In order to assure that the established FDI conditions based on the limit sets of residual-bounding zonotopes can guarantee FDI, one should not use the non-diagonal elements with 1 of the matrix (5.14) to establish guaranteed FDI conditions, which will be detailed in the following contents. For the sake of explaining how to establish these FDI conditions, one takes the following matrix $\mathcal{I}$ as an example, i.e.,

$$\mathcal{I} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \tag{5.15}$$

The example in (5.15) considers four modes corresponding to the four rows of the matrix, respectively. Moreover, four interval observers are designed to monitor these four modes. According to the aforementioned analysis, the system information of the example (5.15) useful for FDI can be described by a new matrix

$$\mathcal{I}' = \begin{bmatrix} 1 & \mathit{0} & 0 & 0 \\ \times & \mathit{1} & 0 & \times \\ \times & \times & 1 & \times \\ \times & 0 & 0 & 1 \end{bmatrix}. \tag{5.16}$$

In this example, if one wants to guarantee that all the four modes are detectable and isolable after their occurrences, it should be assured that any two rows of the matrix $\mathcal{I}'$ in (5.16) are distinguishable. Notice that when verifying the distinguishability of the four modes, one does not consider the entries with $\times$ of the matrix $\mathcal{I}'$. Instead, only the entries with 0 or 1 are considered. Moreover, one cares about the columns (only columns without containing entries with $\times$) of any two rows, as long as there exists one column of the two rows whose two entries are different (i.e., one is 0 and

the other one is 1), it is guaranteed that the modes corresponding to these two rows are detectable and isolable. One takes Row 0 and 1 of the matrix $\mathcal{I}'$ as an example. It can be observed that the 1-st column of the two rows are composed of 0 and 1 (i.e., the italic elements of the matrix $\mathcal{I}'$). Thus, with residual zonotopes estimated by the first interval observer, Mode 0 and 1 can be distinguished by testing the inclusion between the residual zonotopes and the origin and do not need to use residual zonotopes from the other interval observers, which can reduce complexity. This means that, only by using these two entries of Column 1, Row 0 and 1 (i.e., Mode 0 and 1) can be distinguished. Based on the same principle, for any other rows, one can make the similar analysis to see whether or not they are distinguishable. To summarize, it can be observed that one can further distinguish Row 0 and 2 with Column 2, Row 0 and 3 with Column 3, Row 1 and 2 with Column 2, Row 1 and 3 with Column 1 and Row 2 and 3 with Column 2, respectively.

Remark 5.8. *For simplicity, in this chapter, one takes the example* (5.16) *to show the principle of the FDI conditions of the proposed FDI approach. Thus, for real applications, one should obtain the corresponding matrices* $\mathcal{I}$ *and* $\mathcal{I}'$ *and use the method shown in this example to analyze whether or not all considered modes (healthy or faulty) are detectable and isolable.*

Thus, based on the principle shown by the example (5.16), the FDI conditions for the proposed FDI approach are established in the following proposition.

Proposition 5.1. *For all the considered modes (healthy or faulty), a matrix* $\mathcal{I}$ *as in* (5.15) *corresponding to residual-bounding zonotopes can be obtained. Furthermore, based on the matrix* $\mathcal{I}$*, a simplified matrix* $\mathcal{I}'$ *as in* (5.16) *can be obtained. If for any two rows in the matrix* $\mathcal{I}'$*, there exists one column of them without* $\times$ *entries, whose two column entries are different from each other, the two modes corresponding to these two rows are detectable and isolable after their occurrences.*

Proof : If Proposition 5.1 holds, it implies that any two rows in the matrix $\mathcal{I}'$ have at least one common column whose two column elements are different from each other (i.e., one is 0 and the other one is 1). Since one column corresponds to one interval observer, it implies if the system is in either of two modes corresponding to the two rows, residual zonotopes from the interval observer can only always either include or exclude the origin. Thus, by testing the inclusion of residual zonotopes estimated by the interval observer and the origin, the switching between the two modes are detectable and the two modes can be distinguished. □

Thus, if there is an FDI algorithm that can identify the differences of any two modes described in Proposition 5.1, it implies that Proposition 5.1 can be used as guaranteed FDI conditions of this FDI algorithm which will be proposed in the next section.

5.5 Fault Detection and Isolation

This section proposes an algorithm to implement sensor FDI under the FDI conditions proposed in Proposition 5.1.

5.5.1 Fault Detection

To explain the proposed FD principle, it is assumed that the system is in the i-th mode. Thus, a vector $\mathbf{R}_k$ composed of residual zonotopes estimated by all the interval observers can be obtained in real time. If the system operates at steady state of the i-th mode, residual zonotopes estimated by all the interval observers are bounded by the limit sets of residual-bounding zonotopes corresponding to the i-th mode, i.e.,

$$\mathbf{R}_k \subseteq \mathbf{M}^i, \quad i \in \mathbb{I}. \tag{5.17}$$

Thus, whenever (5.17) is violated elementwise, it implies that a fault has occurred.

Additionally, after the system enters into the steady-state operation of the i-th mode, residual zonotopes estimated by the interval observers can be used to test

$$\mathbf{0} \in \mathbf{R}_k, \tag{5.18}$$

where (5.18) should be understood elementwise. After testing (5.18) at each time instant, one can obtain an $(M+1)$-dimensional fault signature vector $\mathcal{F}_i$ (i denotes that, before FD, the system is in the i-th mode) full of 0 and 1, where, as in (5.14), 0 denotes that residual zonotopes estimated by the interval observer corresponding to the vector entry with 0 do not contain the origin while 1 has the opposite explanation. Thus, for FD, one should compare this real-time vector with the i-th row of the matrix $\mathcal{I}'$ (note that the elements with $\times$ of this row should be omitted). If this real-time obtained vector matches the i-th row of the matrix $\mathcal{I}'$, it is considered that the system is still in the i-th mode. Otherwise, it means that a fault has occurred.

Remark 5.9. *In additional, a criteria simpler than* (5.18) *can also be used to detect faults at steady state of the i-th mode, i.e., testing whether or not*

$$\mathbf{0} \in R_k^{ii} \tag{5.19}$$

holds. However, under the FDI conditions in Proposition 5.1, (5.19) *is sufficient but not necessary for FD of all the considered modes. Thus, if* (5.19) *is violated, it means that the system becomes faulty. Otherwise, one cannot assure whether or not a considered mode switching has occurred. This implies that* (5.19) *may only be able to detect parts of the considered modes. Instead, under the FDI conditions in Proposition 5.1,* (5.18) *can detect all the considered modes. Thus, at each time instant, for simplicity, one can first test the i-th component* (5.18) *(i.e.,* (5.19)*) to make a quick FD decision. If* (5.19) *is violated, it implies a model switching. Otherwise, then test the rest of components of* (5.18) *to confirm whether or not a mode switching has occurred.*

Proposition 5.2. *If the system is at steady-state regime of its i-th mode, FD can be performed by simultaneously testing* (5.17) *and* (5.18)*. As long as either of them detects anomaly, it implies that a fault has occurred. Otherwise, it is considered that the system is still in the i-th mode.*

It is known that testing (5.17) or (5.18) allows to implement FD. But, based on the FDI conditions proposed in Proposition 5.1, it is not known whether the FD strategy (5.17) can guarantee that all the considered modes are detectable or not. However, the FD strategy (5.18) can guarantee that all the considered modes are detectable. If one chooses to test both of them on-line for FD, this combination may be more sensitive to some faults. But, the combination has high computational complexity. Besides, an alternative choice is that only the FD strategy (5.18) is used in the proposed FD approach, which has less computational complexity. Thus, for applications, the designers can make a selection between these two ways according to the particular requirements.

5.5.2 Fault Isolation

In this chapter, the proposed FI algorithm is based on residual zonotopes and residual-bounding zonotopes, which is also composed of two FI strategies (transient-state and steady-state). In this subsection, these two FI strategies are presented, respectively.

In order to explain the proposed FI algorithm, it is assumed that the system is at steady state in the i-th mode and a fault is detected at time instant k_d, which implies that the system switches to a new mode different from the i-th one after FD. At the FD time k_d, residual zonotopes $R_{k_d}^{fj}$ ($f \in \mathbb{I}_i = \mathbb{I} \setminus \{i\}$) can always be obtained, where f denotes the index of a new and unknown mode.

As per Proposition 2.1, it is known that, using a starting set to initialize (5.11) at any time, a set sequence can be generated by iterating the dynamics. As k tends to infinity, the set sequence finally converges to a fixed set (i.e., the mRPI set $\check{X}_{\infty}^{ij}$ of $\tilde{X}_k^{ij}$ indicated in (5.7) for the j-th interval observer in the i-th mode).

Thus, at the FD time k_d, by initializing all the dynamics (5.11) corresponding to each interval observer ($j \in \mathbb{I}_i$) with a starting set, a group of set sequences can be generated and a group of the corresponding residual-bounding zonotope sequences can be simultaneously obtained by using (5.10). In this chapter, a starting set for the j-th interval observer in the f-th mode is denoted as $\bar{X}_{k_d}^{fj}$. Thus, a collection of starting sets should be constructed to initialize the corresponding set-based dynamics (5.11), each of which corresponds to one interval observer.

Remark 5.10. *Although residual-bounding zonotope sequences corresponding to all the interval observers under all the considered modes can be generated by using the corresponding starting sets at the FD time k_d, the proposed FI approach only uses the M residual-bounding zonotope sequences $\check{R}_k^{jj}$ ($k \geq k_d$ and $j \in \mathbb{I}_i$) for less complexity.*

By means of the dynamics (5.11), with the corresponding starting sets at the FD time k_d, the set sequences $\check{X}_k^{jj}$ ($k \geq k_d$ and $j \in \mathbb{I}_i$) can be generated, which will always contain state estimation error sets $\tilde{X}_k^{jj}$ ($k \geq k_d$) according to Remark 5.5 if the current mode is also the j-th one. Furthermore, by using (5.10), the corresponding residual-bounding zonotope sequences $\check{R}_k^{jj}$ ($k \geq k_d$ and $j \in \mathbb{I}_i$) can be computed, respectively.

The generated residual-bounding zonotope sequence $\check{R}_k^{jj}$ ($k \geq k_d$) will always contain the residual zonotopes estimated by the j-th interval observer if the current system is also in the j-th mode. However, if the current system is not in the j-th mode, the sequence $\check{R}_k^{jj}$ ($k \geq k_d$) may not contain the residual zonotopes R_k^{fj} ($k \geq k_d$) even at the FD time k_d. This can be explained by the fact that residual-bounding zonotopes depend on the system modes (see (5.10)). At time instant k_d, even though the starting sets of (5.11) for all the interval observers $j \in \mathbb{I}_i$ respectively satisfy

$$\bar{X}_{k_d}^{fj} \supseteq \tilde{X}_{k_d}^{fj}, \quad f \neq i, \tag{5.20}$$

it cannot still guarantee $\check{R}_{k_d}^{jj} \supseteq R_{k_d}^{fj}$, where $\check{R}_{k_d}^{jj}$ is computed as

$$\check{R}_{k_d}^{jj} = G_j C \bar{X}_{k_d}^{fj} \oplus V \oplus (-V). \tag{5.21}$$

Thus, whenever a fault is detected, the proposed transient FI strategy generates M residual-bounding zonotope sequences $\check{R}_k^{jj}$ ($k \geq k_d$ and $j \in \mathbb{I}_i$), each of which corresponds to one candidate mode. This implies that, among the M residual-bounding zonotope sequences, there exists at least one (i.e., the one matching the current after-fault mode) that can always contain the residual zonotopes estimated by its corresponding interval observer for all $k \geq k_d$. Based on this fact, the proposed transient-state FI strategy is summarized as follows.

In the i-th mode, when a fault is detected at the FD time k_d, M residual-bounding zonotope sequences described by the candidate-mode set $\mathbb{I}_i$ can be generated by initializing (5.11) with their corresponding starting sets and using (5.10), the transient-state FI strategy consists in searching a mode by testing whether or not

$$R_k^{fj} \subseteq \check{R}_k^{jj}, \quad j \in \mathbb{I}_i, \quad \text{for all } k \geq k_d \tag{5.22}$$

holds in real time. If a violation of (5.22) corresponding to the j-th interval observer is detected, one immediately stops generating its corresponding residual-bounding zonotope sequence and removes the index j from the candidate-mode set $\mathbb{I}_i$. Testing and removing are repeated until the time instant when the set $\mathbb{I}_i$ remains only one element or the time window used to describe the transition completely elapses. This time instant and this unique element indicates the FI time and fault, respectively.

Remark 5.11. *Since sensor faults can immediately affect the system outputs, this means that a sensor fault is possible to be isolated by the FI strategy proposed in* (5.22) *at the FD time instant* k_d *(see* (5.20) *and* (5.21)*).*

This means that, by using the FI strategy, the FI decision perhaps can be directly obtained by initialization at time instant k_d.

Remark 5.12. *It is possible that, even though the proposed transient-state FI algorithm is persistently executed, there always exist at least two elements in $\mathbb{I}_i$ during the corresponding time window. This implies that accurate FI may not be obtained only by the proposed transient-state FI during the transition. In this chapter, in order to describe the transition induced and the persistent time of the use of this transient-state FI strategy, a proper time window should be defined in advance.*

In order to avoid the situation indicated in Remark 5.12, one also proposes a steady-state FI strategy to complement the transient-state FI strategy by using residual zonotopes and testing the inclusion between residual zonotopes and $\mathbf{0}$ after the time window. By testing these inclusions, one can obtain the fault signature vector $\mathcal{F}_i$. Finally, by matching the matrix $\mathcal{F}_i$ with the rows of the matrix $\mathcal{I}'$, if one row of the matrix $\mathcal{I}'$ can match $\mathcal{F}_i$, then the index of this row indicates the new mode. This steady-state FI strategy is summarized in Proposition 5.3.

Proposition 5.3. *After applying the transient-state FI strategy over a defined time window, if there still exist at least two elements in $\mathbb{I}_i$, FI can still be guaranteed by searching an unique row of the matrix $\mathcal{I}'$ that can match the fault signature vector $\mathcal{F}_i$ and the FI decision is indicated by the index of this row.*

Proof : Under Proposition 5.1, as k tends to infinity, all residual-bounding zonotope sequences converge to their corresponding fixed sets (i.e., the elements of the matrix $\mathbf{M}$). Since if residual-bounding zonotope sequences do not contain $\mathbf{0}$, it is guaranteed that its corresponding residual zonotopes in Table 5.1 at steady state do not contain $\mathbf{0}$ too. Moreover, in the case that an interval observer matches the current system mode, the residual zonotopes estimated by this interval observer can contain $\mathbf{0}$ at steady state. This implies that, under Proposition 5.1, the fault signature vector $\mathcal{F}_i$ is different in different modes and can match one and only one row of the matrix $\mathcal{I}'$. Thus, FI can be guaranteed by comparing $\mathcal{F}_i$ with the rows of the matrix $\mathcal{I}'$ on-line. □

In order to explain how to obtain the fault signature vector $\mathcal{F}_i$, one still uses the example given by (5.15) and (5.16). Firstly, one assumes that the system is in the healthy mode at the beginning, after a fault is detected, one knows that all the faults 1, 2 and 3 are candidates. With the matrix (5.16), it can be observed that the faults 1 and 2 can be distinguished by using residual zonotopes estimated by the observer 2, the faults 1 and 3 by the observer 1 and the faults 2 and 3 by the observer 2. This means that, after a fault is detected, one only needs to use residual zonotopes estimated by the interval observers 1 and 2, while the other two interval observers 0 and 3 are not necessary to use. Thus, from the computational point of view, $\mathcal{F}_0$ should be a two-dimensional vector whose elements are composed of the binary information by testing inclusion between residual zonotopes estimated by the interval observers 1 and 2 and the origin.

But, for simplicity, one can always define $\mathcal{F}_0$ as a four-dimensional vector, whose four elements are obtained by testing inclusion between residual zonotopes estimated by all the four interval observers and the origin. But, finally, only the 1-st and 2-nd elements of $\mathcal{F}_0$ are used to compare with the 1-st and 2-nd elements of Row 1, 2 and 3 of the matrix (5.16) for FI, while the 0-th and 3-rd elements of $\mathcal{F}_0$ are not useful.

Remark 5.13. *In this chapter, the whole FI algorithm simultaneously includes the two FI strategies respectively presented in (5.22) and Proposition 5.3. The former may be able to isolate faults during the transition but without FI guarantees, while the latter with FI guarantees requires longer FI time after the transition.*

5.5.3 Starting Sets for Fault Isolation

In Section 5.5.2, it can be observed that the starting sets for residual-bounding zonotope sequences are crucial for the transient-state FI strategy. An idea to construct these starting sets is given. Firstly, by using a zonotope $V_0 = H_{\bar{\eta}}\mathbb{B}^q$, in the unknown mode f, for the j-th interval observer, the corresponding residual zonotope indicated in (5.4) can be transformed into

$$R_{k_d}^{fj} = G_j C\tilde{X}_{k_d}^{fj} \oplus \{(G_f - G_j)Cx_{k_d}\} \oplus \{\eta_{k_d} - \eta^c\} \oplus (-V_0). \tag{5.23}$$

By adding $-(\eta_{k_d} - \eta^c)$ and $-(G_f - G_j)Cx_{k_d}$ to both sides, the previous equation turns into

$$R_{k_d}^{fj} \oplus \{-(\eta_{k_d} - \eta^c)\} \oplus \{-(G_f - G_j)Cx_{k_d}\} = G_j C\tilde{X}_{k_d}^{fj} \oplus (-V_0). \tag{5.24}$$

Considering $\eta_{k_d} - \eta^c \in V_0$ and $x_{k_d} \in X$, one further has

$$G_j C\tilde{X}_{k_d}^{fj} \oplus (-V_0) \subseteq R_{k_d}^{fj} \oplus (-V_0) \oplus (G_j - G_f)CX. \tag{5.25}$$

Since V_0 can be removed from both sides of the equation, one can obtain

$$G_j C\tilde{X}_{k_d}^{fj} \subseteq R_{k_d}^{fj} \oplus (G_j - G_f)CX. \tag{5.26}$$

It can be observed that the right side of (5.26) is dependent of modes. But, before the fault is isolated, it is not possible to know the new mode. Thus, one should construct initial sets without being affected by modes. Here, one has to consider three different cases.

- If $j \neq f$ and $j = 0$, one always has

  $$G_j - G_f = \text{diag}(0, \ldots, 0, 1 - g_f, 0, \ldots, 0).$$

  where g_f is the f-th diagonal element of G_f that models the f-the sensor fault.

- If $j \neq f$ and $j \neq 0$, one always has

$$G_j - G_f = \text{diag}(0, \ldots, 0, g_j - 1, 0, \ldots, 0, 1 - g_f, 0, \ldots, 0),$$

  where g_j is the j-th diagonal element of G_j that models the j-the sensor fault.

- If $j = f$, one always has

$$G_j - G_f = 0.$$

By summarizing the aformentioned three cases, one can obtain that, if $j = 0$, one always has

$$G_j - G_f \in G_{fj} = \text{diag}([0, 1 - g_1], [0, 1 - g_2], \ldots, [0, 1 - g_q]),$$

while if $j \neq 0$, one always has

$$G_j - G_f \in G_{fj} = \text{diag}([0, 1 - g_1], \ldots, [0, 1 - g_{j-1}], 1 - g_j, [0, 1 - g_{j+1}], \ldots, [0, 1 - g_q]).$$

where G_{fj} is a diagonal interval matrix that can always include $G_j - G_f$ inside its interval as long as the mode switching from the j-th mode occurs. Thus, one can further have

$$(G_j - G_f)CX \subseteq G_{fj}CX, \tag{5.27}$$

where, considering that X is a zonotope and G_{fj} is an interval matrix, with Properties 2.6 and 2.7, $G_{fj}CX$ can be over-approximated by a zonotope denoted as

$$Z^{fj} = z^{fj,c} \oplus H_z^{fj} \mathbb{B}^{s^{fj}},$$

where s^{fj} is the order of Z^{fj}. Thus, in order to remove the effect of modes, a solution is to further transform (5.26) into

$$G_j C \tilde{X}_{k_d}^{fj} \subseteq R_{k_d}^{fj} \oplus Z^{fj}. \tag{5.28}$$

Since $R_{k_d}^{fj}$ is zonotope, the term $R_{k_d}^{fj} \oplus Z^{fj}$ can be rewritten into the zonotopic form

$$R_{k_d}^{fj} \oplus Z^{fj} = r_{k_d}^{fj,c} \oplus H_{k_d}^{fj,r} \mathbb{B}^{s_{k_d}^{fj,r}}, \tag{5.29}$$

where $s_{k_d}^{fj,r}$ is the zonotope order, and $r_{k_d}^{fj,c}$ and $H_{k_d}^{fj,r}$ can be respectively derived as

$$r_{k_d}^{fj,c} = y_{k_d} - \hat{y}_{k_d}^{c,y} + z^{fj,c}, \tag{5.30a}$$

$$H_{k_d}^{fj,r} = [\hat{H}_{k_d}^{j,y} \;\; H_z^{fj}]. \tag{5.30b}$$

With the help of the zonotopic form of $R_{k_d}^{fj} \oplus Z^{fj}$, (5.28) is rewritten as

$$G_j C \tilde{X}_{k_d}^{fj} \oplus \{-r_{k_d}^{fj,c}\} \subseteq H_{k_d}^{fj,r} \mathbb{B}_{k_d}^{s^{fj,r}}. \tag{5.31}$$

Using $F(l)$, $H_{k_d}^{fj,r}(l)$ and $r_{k_d}^{fj,c}(l)$ to denote the l-th rows of G_jC and $H_{k_d}^{fj,r}$ and the l-th component of $r_{k_d}^{fj,c}$, respectively, one can obtain a group of inequalities corresponding to (5.31), where the l-th inequality can be written as

$$| F(l)\tilde{x}_k^{fj} - r_{k_d}^{fj,c}(l) | \leq \| H_{k_d}^{fj,r}(l) \|_1, \; l = 1, 2, \cdots, q, \tag{5.32}$$

where $\tilde{x}_k^{fj}$ represents the elements that satisfy (5.32).

Remark 5.14. *It can be observed that the description* (5.32) *is more conservative than* (5.31)*, which means, if the q inequalities of* (5.32) *can determine a closed set, the closed set can fully contain $\tilde{X}_{k_d}^{fj}$ in* (5.31)*.*

Assumption 5.4. *For the j-th interval observer, $\tilde{X}^j$ denotes a given zonotope determined by the physical constraints of the system and can always bound $\tilde{X}_k^{ij}$ for all $i \in \mathbb{I}$.*

As per Property 2.4, each inequality out of the q inequalities of (5.32) generally determines a strip and the q inequalities together can form a closed set that contains $\tilde{X}_{k_d}^{fj}$. However, there exist two possible cases that depend on the system dynamics.

- If the q inequalities themselves can form a closed set, this set can contain $\tilde{X}_{k_d}^{fj}$,
- If the q inequalities cannot form a closed set (i.e., there are not enough strips such that their intersection cannot lead to a closed set), then $\tilde{X}^j$ indicated in Assumption 5.4 can be further used to construct a closed set that can contain $\tilde{X}_{k_d}^{fj}$.

However, because Property 2.4 can only compute a zonotope approximation of the intersection of a zonotope and a strip, for the j-th interval observer, $\tilde{X}^j$ has to be used as the initial zonotope of Property 2.4 for both cases. As seen in Section 5.5.2, for the j-th interval observer, the constructed starting zonotope for the residual-bounding zonotope sequence is denoted as $\bar{X}_{k_d}^{fj}$.

Remark 5.15. *In a particular case, if the matrix G_jC is invertible,* (5.28) *can be directly transformed into*

$$\tilde{X}_{k_d}^{fj} \subseteq (G_jC)^{-1}\{R_{k_d}^{fj} \oplus Z^{fj}\}, \tag{5.33}$$

where $(G_jC)^{-1}$ denotes the inverse of G_jC and $(G_jC)^{-1}\{R_{k_d}^{fj} \oplus Z^{fj}\}$ is directly used as the starting set $\bar{X}_{k_d}^{fj}$.

At the FD time k_d, the proposed FI approach constructs a group of starting sets for generating M corresponding residual-bounding set sequences $\check{R}_k^{jj}$ ($j \in \mathbb{I}_i$). As derived before, for the j-th interval observer, its residual-bounding set sequence is generated by initializing its corresponding dynamics (5.11) with the starting set

$$\check{X}_{k_d}^{jj} = \bar{X}_{k_d}^{fj}, \;\; \text{for all} \;\; j \in \mathbb{I}_i. \tag{5.34}$$

As said in Remark 4.13, one can also use Property 2.5 to construct the starting sets. However, there is a difference in the case of sensor faults, which is that, for each interval observer, one should construct a starting set. Thus, totally, one should construct M starting sets at one time for M interval observers corresponding to all candidate modes.

5.5.4 Fault Detection and Isolation Algorithm

According to the aforementioned discussions, based on the FDI conditions in Proposition 5.1, faults can be detected by Proposition 5.2. Whenever a fault is detected, after applying the proposed FI strategies in (5.22) and Proposition 5.3, theoretically, the worst case is that the fault can only be isolated at infinity because the FDI conditions are built by means of the limit sets of residual-bounding zonotopes. However, from the practical point of view, it is impossible to obtain residual-bounding zonotopes at infinity. Thus, in order to establish the proposed FDI conditions and implement the proposed FDI approach, one has to consider the RPI approximations of the limit sets (i.e., $\check{R}_{\infty}^{ij}$) of residual-bounding zonotopes.

According to Theorem 2.1, for the set-based dynamics (5.11), the mRPI set $\check{X}_{\infty}^{ij}$ can be approximated by an RPI set $\mathring{X}^{ij}$ with an arbitrarily approximate precision to $\check{X}_{\infty}^{ij}$. Thus, the set $\check{R}_{\infty}^{ij}$ can be approximated by the corresponding set

$$\mathring{R}^{ij} = G_j C \mathring{X}^{ij} \oplus (G_i - G_j) CX \oplus V \oplus (-V). \tag{5.35}$$

One should notice that whenever $\tilde{X}_k^{ij}$ goes into and stays inside $\mathring{X}^{ij}$, R_k^{ij} also goes into and stays inside $\mathring{R}^{ij}$. Since all RPI sets (i.e., $\mathring{R}^{ij}$) can be computed off-line, all entries of Table 5.2 is over-approximated by Table 5.4.

Table 5.4: RPI sets of residual zonotopes

	Interval Observer 0	$\cdots$	Interval Observer i	$\cdots$	Interval Observer M
Mode 0	$\mathring{R}^{00}$	$\cdots$	$\mathring{R}^{0i}$	$\cdots$	$\mathring{R}^{0M}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode i	$\mathring{R}^{i0}$	$\cdots$	$\mathring{R}^{ii}$	$\cdots$	$\mathring{R}^{iM}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode M	$\mathring{R}^{M0}$	$\cdots$	$\mathring{R}^{Mi}$	$\cdots$	$\mathring{R}^{MM}$

According to the definition of the mRPI set in Definition 2.18, $\check{X}_{\infty}^{ij} \subseteq \mathring{X}^{ij}$ and $\check{R}_{\infty}^{ij} \subseteq \mathring{R}^{ij}$ hold. This implies that after initializing (5.11), the set sequence of the corresponding residual-bounding zonotopes will finally enter into and stay inside its corresponding set (i.e., $\mathring{R}^{ij}$) as k increases.

Algorithm 2 FD algorithm

Require: $\hat{X}_0$, $\mathbb{I}$ and current mode index $i \in \mathbb{I}$;
Ensure: f;
1: Interval observer initialization: $\hat{X}_0^{ij} = \hat{X}_0$ (for all $j \in \mathbb{I}$);
2: At time instant k: No fault alarm and $f \leftarrow$ FAULT;
3: **while** $f \neq$ TRUE **do**
4: $k \leftarrow k + 1$;
5: Obtain $\mathbf{R}_k$;
6: **if** (5.17) or (5.18) makes a fault alarm **then**
7: $f \leftarrow$TRUE;
8: **end if**
9: **end while**
10: **return** f;

Thus, as long as the given approximate precision is sufficiently high, Table 5.4 can be used to replace Table 5.2 for verifying the FDI conditions in Proposition 5.1. Moreover, Table 5.3 can be derived from Table 5.4. Furthermore, based on Table 5.4, for the i-th mode, one defines a vector

$$\mathring{\mathbf{R}}^i = (\mathring{R}^{i0}, \mathring{R}^{i1}, \cdots, \mathring{R}^{iM}), \tag{5.36}$$

which is used for Algorithm 2 to carry out the FD strategy. The proposed FI algorithm is a combination of the two FI strategies presented in (5.22) and Proposition 5.3. Practically, once a fault is detected, this FI algorithm firstly starts up the FI strategy as in (5.22). If the FI strategy in (5.22) cannot isolate the fault within a defined time window, the FI algorithm will terminate it and then the FI strategy in Proposition 5.3 is started to guarantee FI at steady state. Thus, in this FI algorithm, the defined time window for the transient-state FI strategy is used as a switching mechanism between the two FI strategies in (5.22) and Proposition 5.3.

According to (5.11), after the initialization required to obtain residual-bounding zonotope sequences on-line, the differences between the set values of residual-bounding zonotopes at different time instants are dependent of the term $(A - L_j G_j C)\check{X}_k^{ij}$, i.e., the eigenvalues of $A - L_j G_j C$ and the starting set of initialization. Because all eigenvalues of $A - L_j G_j C$ are inside the unit circle, after the transition induced by a mode switching, all residual-bounding zonotope sequences finally enter into steady state and can sufficiently and asymptotically approximate their corresponding limit sets. This implies that, at steady state, the difference between the set values of a residual-bounding zonotope sequence at different time instants will gradually decrease. This fact allows to define a proper time window as mentioned in Remark 5.12 as the switching mechanism between the two FI strategies.

Definition 5.1. *The time window T starting from the FD time instant k_d is defined at least as the maximal settling time of the dynamics of all interval observers such that*

the proposed FI strategy in Proposition 5.3 can guarantee FI.

Remark 5.16. *The transitions between different modes are determined by the eigenvalues of the corresponding dynamics. Theoretically, it can also be assessed by the settling time of interval observers. Most importantly, a proper time window can always be selected by a sufficient number of simulations.*

As per Definition 5.1 and Remark 5.16, a mechanism of switching between the proposed FI strategies in (5.22) and Proposition 5.3 is introduced by the time window T and the proposed FI algorithm is summarized as follows:

1. Once a fault is detected by Proposition 5.2, the transient-state FI strategy in (5.22) is firstly started to isolate the fault within the time window T.
2. After T, if the fault is still not isolated, then the first FI strategy is terminated and the FI algorithm starts up the second FI strategy proposed in Proposition 5.3 for FI at steady state .
3. After the second strategy enters in operation, at each time instant, the inclusion between residual zonotopes and $\mathbf{0}$ is tested, and the testing results are used to compare with the off-line inclusion information stored in each row of $\mathcal{I}'$.
4. If at a time instant, the obtained inclusion results (i.e., $\mathcal{F}_i$) match one row of $\mathcal{I}'$, the index of this row indicates the fault (this index is assumed as f).
5. In order to improve reliability of the FI decision given in Step 4, $\mathbf{R}_k \subseteq \mathring{\mathbf{R}}^f$ can also be tested. If $\mathbf{R}_k \subseteq \mathring{\mathbf{R}}^f$ holds, the FI decision of Step 4 can be confirmed. Otherwise the second FI strategy in Proposition 5.3 is repeated again.

Remark 5.17. *Both Steps 4 and 5, respectively considering the invariant set-based and the interval observer-based FI principles, are used to make FI decisions. However, the core step is Step 4, while Step 5 is an assistant step. For simplicity, one can also omit Step 5 and only use Step 4.*

Notice that, the proposed FDI approach is based on the combination of invariant sets and interval observers. By this combination, the conservatism of FDI conditions should be reduced in some sense because of the use of all available system-operating information from all the corresponding interval observers. Comparing with the interval observer-based or the invariant set-based approach, the FDI effectiveness and reliability is possible to be improved.

5.6 Illustrative Example

The second pitch system of a wind turbine benchmark proposed in [43] is used as the case study. Please see [43] for the details of the structure of this pitch system. The

continuous-time dynamics of this subsystem can be found in [61], i.e.,

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{5.37a}$$
$$y(t) = Cx(t). \tag{5.37b}$$

In this subsystem, two sensors are used to measure the pitch position $y(t)$, whose measurements are

$$y_1(t) = G_1(Cx(t) + \eta_1(t)), \tag{5.38a}$$
$$y_2(t) = G_2(Cx(t) + \eta_2(t)), \tag{5.38b}$$

where $y_1(t)$ and $y_2(t)$ denote the measurements of the first and second sensors, respectively, $\eta_1(t)$ and $\eta_2(t)$ are the corresponding measurement noises, G_1 and G_2 model the fault in the first and second sensors, respectively. If G_1 (or G_2) is the identity matrix, it means that the corresponding sensors are healthy. Otherwise, it implies that the corresponding sensors becomes faulty. Besides, the control action is designed as

$$u(t) = u^{ref}(t) + u^f(t), \tag{5.39}$$

where $u^{ref}(t)$ is the given input and $u^f(t)$ is the feedback with a form $u^f(t) = y(t) - 0.5(y_1(t) + y_2(t))$. Furthermore, one can equivalently reformulate (5.37) and (5.38) of the pitch system into a compact form, which describes the pitch system, i.e.,

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{5.40a}$$
$$y_{12}(t) = G_{12}Cx(t) + \eta(t), \tag{5.40b}$$

where

$$y_{12}(t) = \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix}, \; G_{12} = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}, \; \eta_k = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix} \begin{bmatrix} \eta_1(t) \\ \eta_2(t) \end{bmatrix}.$$

The sets of the noises of the sensors are described by $\bar{\eta_1} = 0.8$, ${\eta_1}^c = 0$, $\bar{\eta_2} = 0.8$ and ${\eta_2}^c = 0$, which follows the form of uncertainties in (3.2). The parameters of the second pitch system are given as

$$A = \begin{bmatrix} -13.33 & -123.43 \\ 1 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \; C = \begin{bmatrix} 0 & 123.43 \end{bmatrix}.$$

Remark 5.18. *Since the noises are Gaussian, the aforementioned bounds are empirical values according to the fact that, usual choices for Gaussian distribution, are the band $[-3\sigma, 3\sigma]$ with probability of 99%, or band $[-6\sigma, 6\sigma]$ with probability of 99.99%.*

The sampling time of the pitch system is 0.01s. After discretization, the system parameters are

$$A_d = \begin{bmatrix} 0.867 & -1.234 \\ 0.01 & 1 \end{bmatrix}, B_d = \begin{bmatrix} 0.01 \\ 0 \end{bmatrix}, C_d = \begin{bmatrix} 0 & 123.43 \end{bmatrix}.$$

In this case study, one considers two faults in the two sensors, respectively, and it is assumed that one and only one sensor becomes faulty at any given time (note that one can also consider that two sensors become faulty simultaneously). Thus, the system should have three different sensor modes: healthy, fault in the first sensor and fault in the second sensor, which are respectively modelled as

$$G_{12}^{0} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, G_{12}^{1} = \begin{bmatrix} 0.1 \\ 1 \end{bmatrix}, G_{12}^{2} = \begin{bmatrix} 1 \\ 0.1 \end{bmatrix}.$$

In this chapter, one assumes that the reference input[1] of the pitch system varies in the operating range $u^{ref}(t) \in [10^{\circ},\ 30^{\circ}]$. Furthermore, as per (5.39), by simulating the pitch system with a time span of 10^6s, an empirical bound of $u(t)$ is obtained as $u(t) \in [8.561,\ 52.2314]$. Thus, based on the obtained discrete-time dynamics, Theorem 2.1 and Proposition 2.1, an RPI approximation of the mRPI set of states is constructed by iterating 150 times from an initial state RPI set, which is denoted as

$$X = \begin{bmatrix} 0 \\ 0.2463 \end{bmatrix} \oplus \begin{bmatrix} 2.3934 & 0 \\ 0 & 0.2252 \end{bmatrix} \mathbb{B}^2.$$

Three interval observers are respectively designed to monitor the three modes. The initial state of the system and the initial zonotope of interval observers are respectively given as

$$x_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \hat{X}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathbb{B}^2.$$

In order to obtain guaranteed FDI, one has to check the corresponding FDI conditions in Proposition 5.1. As per Theorem 2.1 and Proposition 2.1, for each mode, the RPI approximations of the limit sets (i.e., $\breve{R}_{\infty}^{ij}$) of the relevant residual-bounding zonotopes, indicated in Table 5.4, are obtained by iterating the dynamics (5.11) 120 times with initial RPI sets of $\tilde{X}_k^{ij}$. These RPI approximations are presented as follows:

- For the healthy mode:

$$\begin{aligned} \mathring{R}^{00} &= ([-3.6507,\ 3.6507], [-3.6507,\ 3.6507])^T, \\ \mathring{R}^{01} &= ([0.7196,\ 53.5725], [-9.0443,\ 4.7407])^T, \\ \mathring{R}^{02} &= ([-9.0443,\ 4.7407], [0.7196,\ 53.5725])^T. \end{aligned}$$

- For the fault in the first sensor:

$$\begin{aligned} \mathring{R}^{10} &= ([-59.8823,\ 26.8929], [-8.2239,\ 29.9569])^T, \\ \mathring{R}^{11} &= ([-0.3651,\ 0.3651], [-3.6507,\ 3.6507])^T, \\ \mathring{R}^{12} &= ([-63.4498,\ 47.4594], [0.4448,\ 58.1507])^T. \end{aligned}$$

[1] In this case study, as an example, the reference input is chosen as a sinusoidal signal.

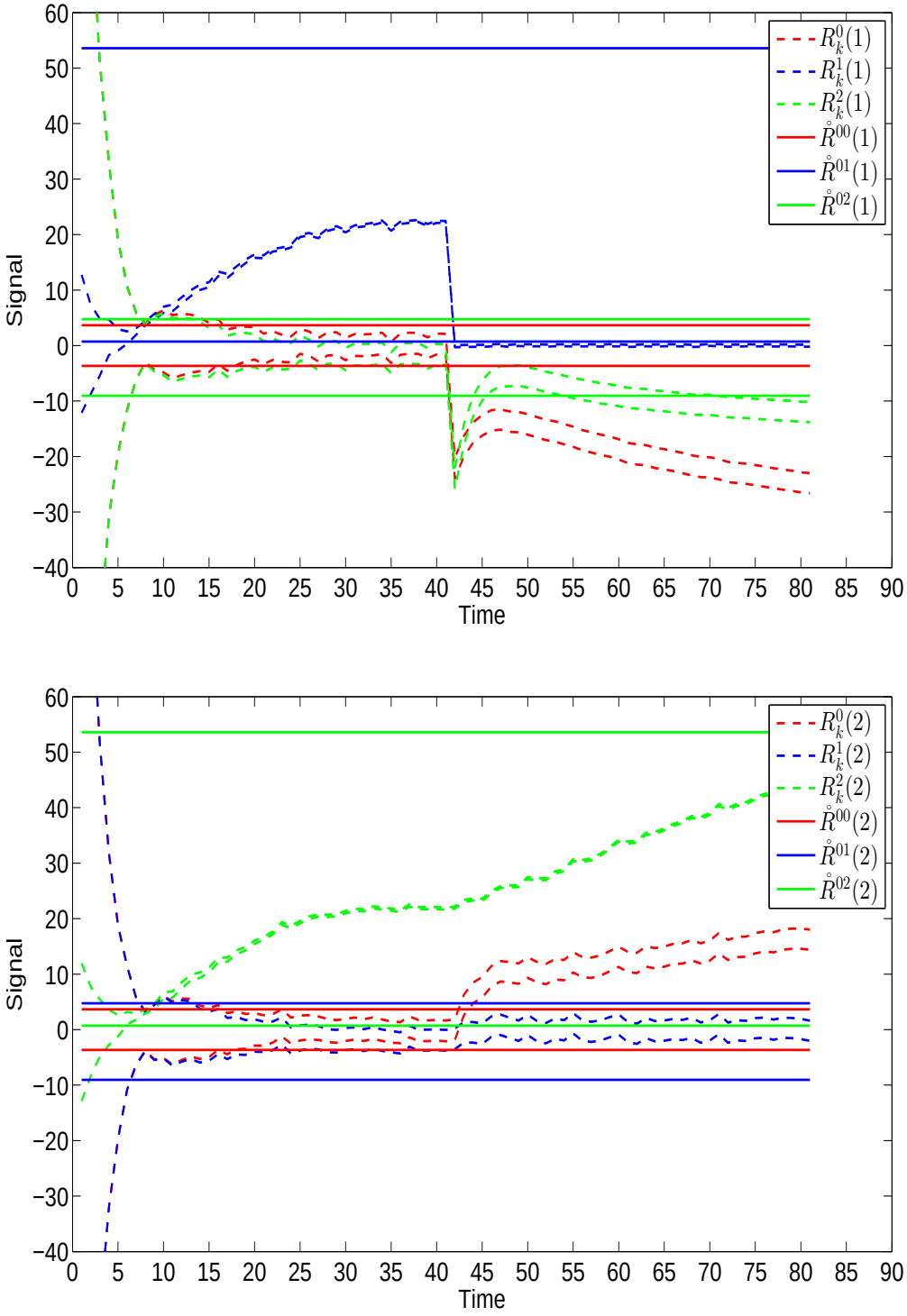


Figure 5.1: FD of Fault 1

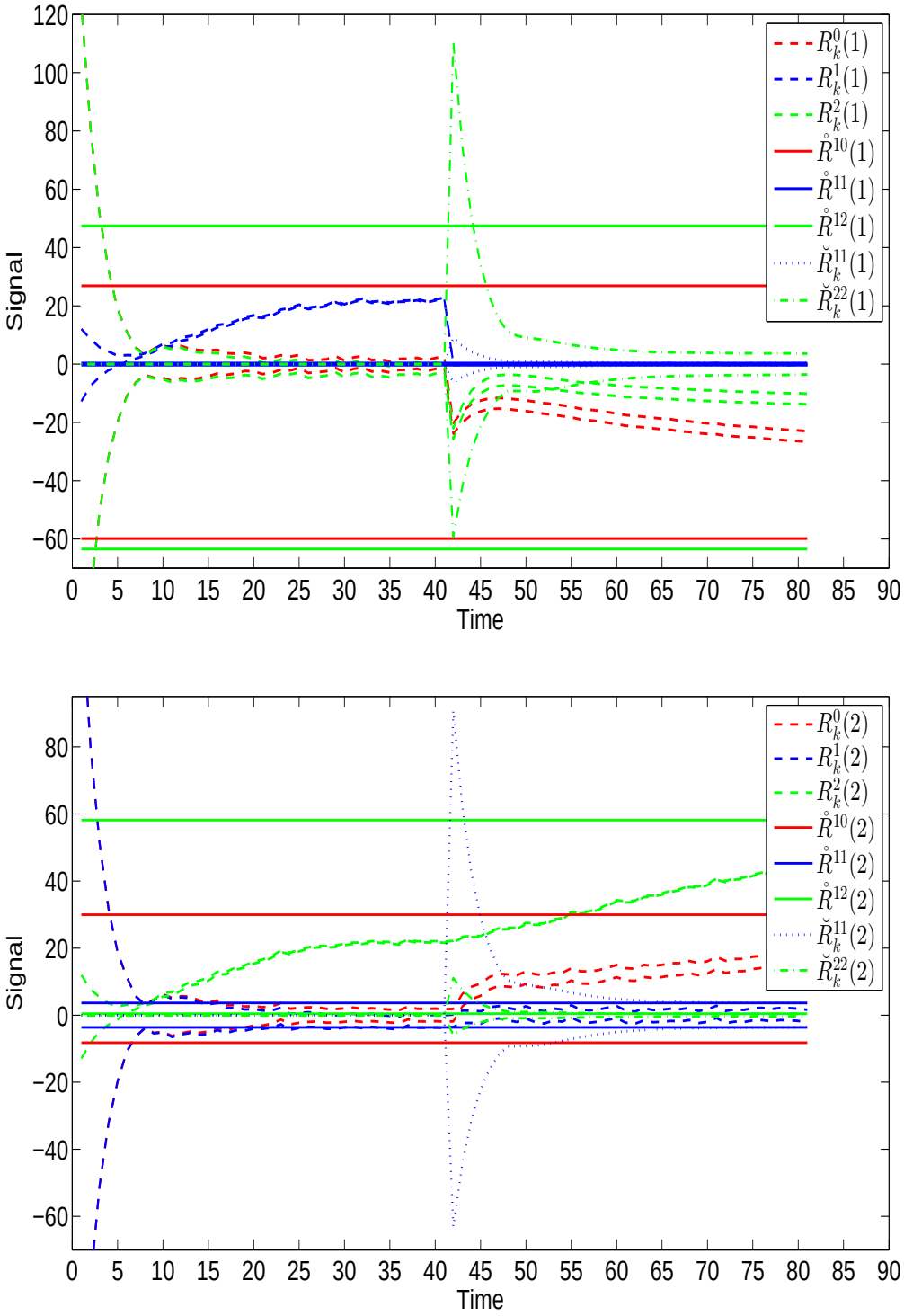


Figure 5.2: FI of Fault 1

- For the fault in the second sensor:

$$\mathring{R}^{20} = ([-8.2239,\ 29.9569], [-59.8823,\ 26.8929])^T,$$
$$\mathring{R}^{21} = ([0.4448,\ 58.1507], [-63.4498,\ 47.4594])^T,$$
$$\mathring{R}^{22} = ([-3.6507,\ 3.6507], [-0.3651,\ 0.3651])^T.$$

Table 5.5: Available off-line system information

	Interval Observer 0	Interval Observer 1	Interval Observer 2
Mode 0	1	0	0
Mode 1	1	1	0
Mode 2	1	0	1

By analyzing these RPI approximations, one can obtain Table 5.5, which collects the off-line system-operating information corresponding to all the different modes and interval observers. Furthermore, based on Table 5.5, one can obtain the matrix $\mathcal{J}'$, which is shown as

$$\mathcal{J}' = \begin{bmatrix} 1 & 0 & 0 \\ \times & \mathbf{1} & \mathit{0} \\ \times & \mathbf{0} & \mathit{1} \end{bmatrix}. \tag{5.41}$$

It can be checked that the matrix $\mathcal{J}'$ in (5.41) satisfies the FDI conditions proposed in Proposition 5.1. As seen in (5.41), all the non-diagonal entries with 1 are omitted. After omiting these entries, it is seen that the three rows of the matrix $\mathcal{J}'$ are different from each other, which means that three modes are distinguishable from each other. Thus, whenever, if a considered mode has occurred, it can be guaranteed that the mode can be detected and then isolated by the proposed FDI approach.

This example only takes the dynamic process of the system from healthy to faulty as an example. Thus, it is not necessary to take Row 0 corresponding to the healthy mode into account in terms of FI of the two sensor faults. According to the FD strategy in Proposition 5.2, at most, R_k^0, R_k^1, R_k^2, $\mathring{R}^{00}$, $\mathring{R}^{01}$ and $\mathring{R}^{02}$ are needed for FD implementation. Moreover, according to the proposed FI strategy in (5.22) and Proposition 5.3, one only needs to obtain R_k^1 or R_k^2 to distinguish the two sensor-fault modes and test the inclusion between the origin and them, respectively. Eventually, FI can be done by comparing the tested inclusion results with the rows of the matrix $\mathcal{J}'$.

According to the FI approach in (5.22), by initializing (5.11), one can obtain the corresponding residual-bounding zonotope sequences $\breve{R}_k^{11}$ and $\breve{R}_k^{22}$ for isolating the faults 1 and 2 during the transient-state operation. But one should notice that the transient-state FI strategy in (5.22) cannot be guaranteed by the FDI conditions in Proposition 5.1. This implies that the transient-state FI strategy may be able to isolate

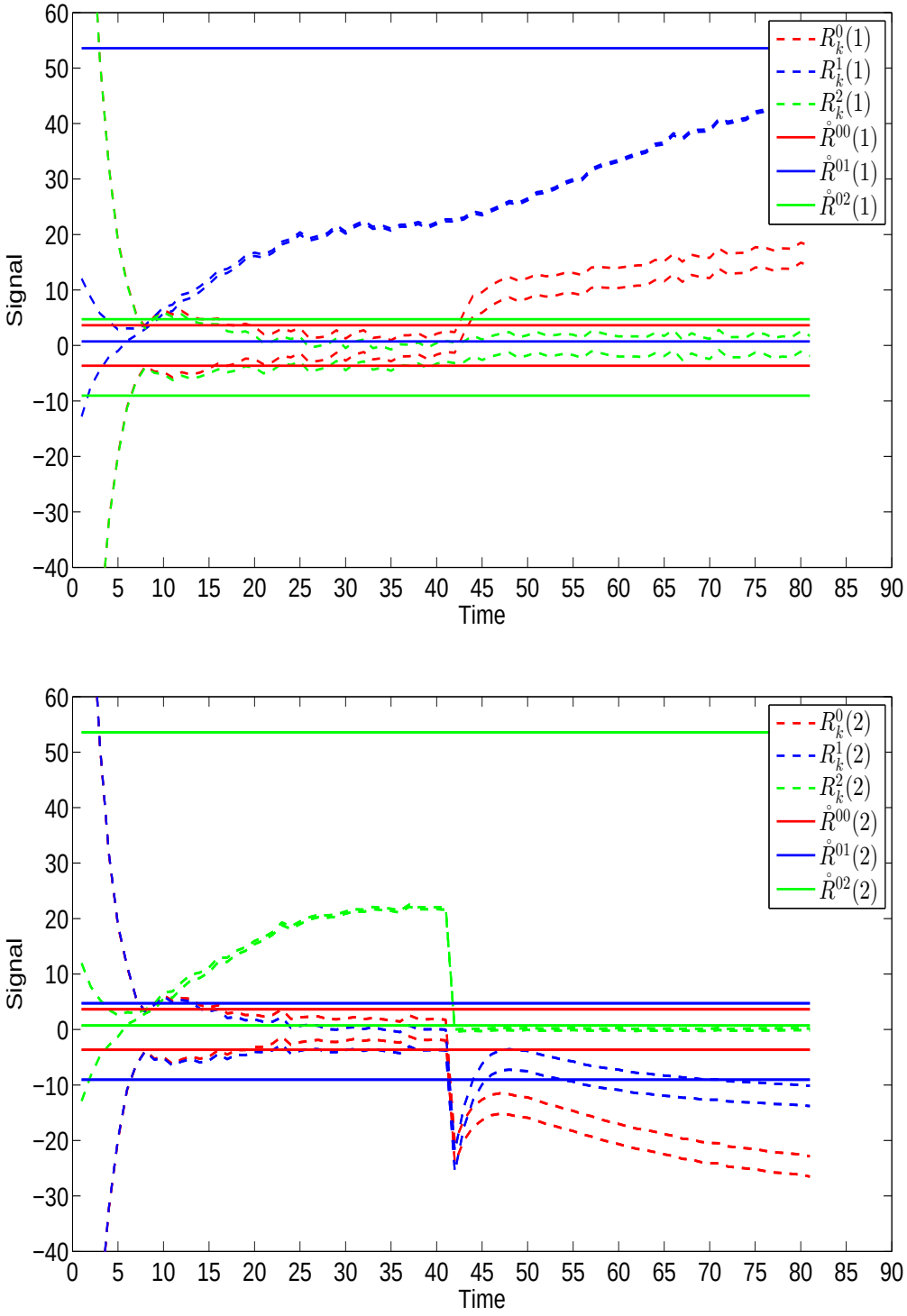


Figure 5.3: FD of Fault 2

faults during the transition or not, which depends on the faults themselves. Besides, the set for the transient-state FI strategy in Assumption 5.4 are given by simulations as

$$\tilde{X}^0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix} \mathbb{B}^2.$$

The time window in Definition 5.1 is given as five steps, and in order to compute the starting zonotopes for the initialization for residual-bounding zonotope sequences, λ in Property 2.4 is given as $\lambda = \begin{bmatrix} 0.005 & 0.005 \end{bmatrix}^T$.

Remark 5.19. *The selection of λ is important for the approach, which affects the volume of the obtained starting zonotopes by Property 2.4. Please see [2] for details.*

In this example, one considers the same scenario for both sensor faults: from time instants 1 to 40, the system is healthy, then a fault occurs at time instant 41 and the system is in the faulty operation from the instants 41 to 80. Thus, the simulations for the two sensor faults are done, respectively, and the diagnostic results of the faults in the first and second sensors are shown in Figures 5.1, 5.2, 5.3 and 5.4.

Remark 5.20. *In the figures, $R_k^i(1)$ and $R_k^i(2)$ denote the first and second components of the residual zonotope R_k^i estimated by the i-th interval observer at time instant k. Similarly, $\mathring{R}^{ij}(1)$ and $\mathring{R}^{ij}(2)$ denote the first and second components of the approximation $\mathring{R}^{ij}$ of R_∞^{ij} corresponding to the j-th interval observer under the i-th mode.*

According to the FD principle in Proposition 5.2 and the results shown in Figure 5.1, it can be observed that a fault is detected at time instant 42 (i.e, $\mathbf{0} \notin R_{42}^0$, $R_{42}^0 \not\subseteq \mathring{R}^{00}$, $R_{42}^1 \not\subseteq \mathring{R}^{01}$ or $R_{42}^2 \not\subseteq \mathring{R}^{02}$). Furthermore, according to the transient-state FI approach in (5.22) and the simulation results shown in Figure 5.2, the first fault is isolated at time instant 42 because of $R_{42}^1 \subseteq \check{R}_{42}^{11}$ and $R_{42}^2 \not\subseteq \check{R}_{42}^{22}$. This indicates that the first fault is isolated at the same time when it is detected, which means no time delay between FD and FI (see Remark 5.11). Additionally, to show the steady-state FI strategy in Proposition 5.3, one should wait a defined five-step time window. Thus, one should test whether or not $\mathbf{0} \in R_{47}^1$ (or/and $\mathbf{0} \in R_{47}^2$) holds. As shown in Figure 5.2, it is seen that $\mathbf{0} \in R_{47}^1$ (or/and $\mathbf{0} \notin R_{47}^2$) holds, which matches Row 1 of the matrix $\mathcal{I}'$. This implies that the fault is in the first sensor, which provides the same FI decision with the transient-state FI strategy.

Remark 5.21. *The size of $\bar{X}_{k_d}^{fj}$ affects the quickness of the transient-state FI proposed in (5.22), but is not decisive. Because, even though the transient-state FI strategy cannot isolate faults within the time window, the proposed FI algorithm can still use the steady-state FI strategy in Proposition 5.3 to guarantee to isolate faults after the time window.*

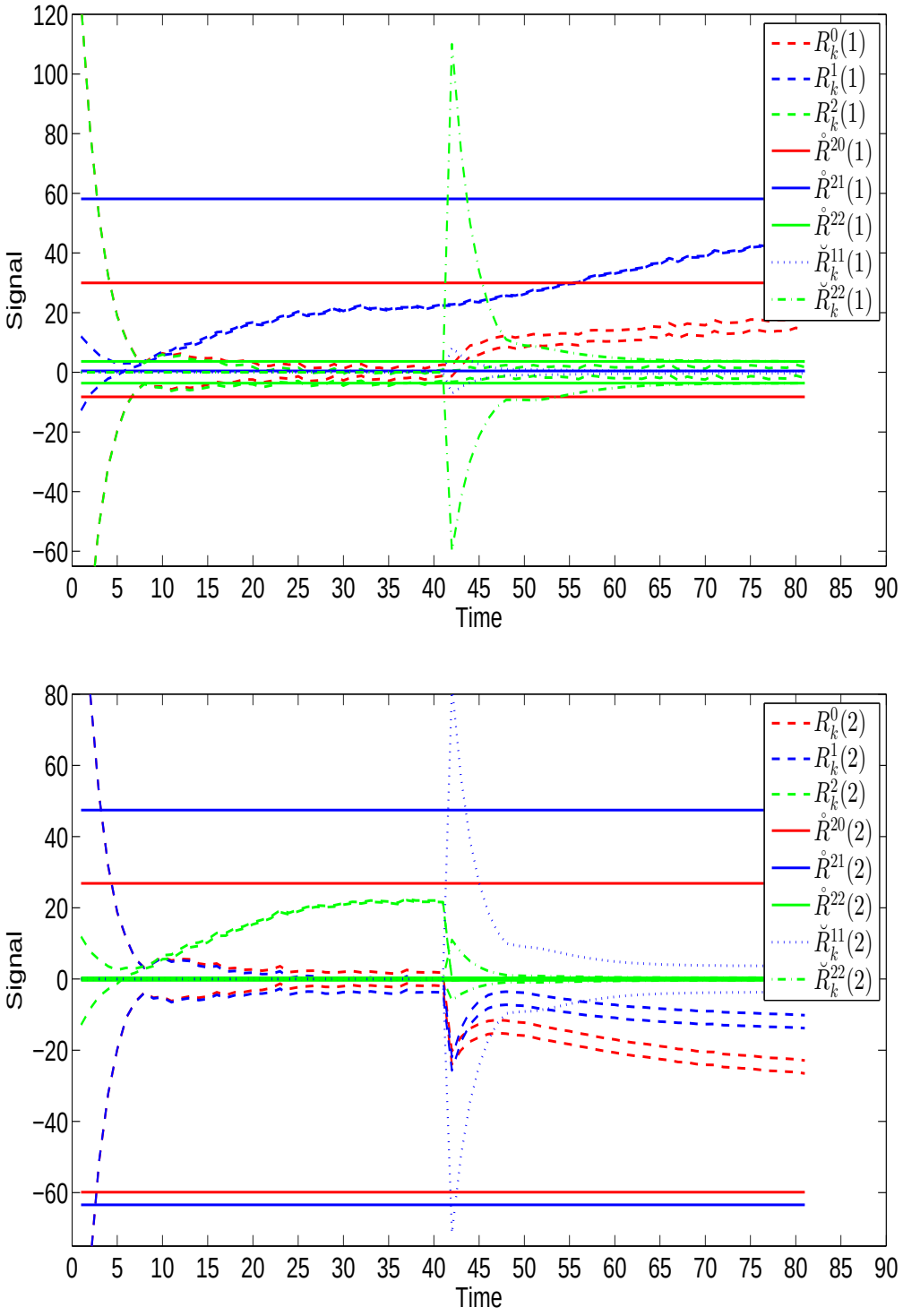


Figure 5.4: FI of Fault 2

Similarly, FDI of the second fault is illustrated in Figures 5.3 and 5.4. In Figure 5.3, it is seen that a fault is detected at time instant 42 (i.e., $\mathbf{0} \notin R_{42}^{0}$, $R_{42}^{0} \nsubseteq \mathring{R}^{00}$, $R_{42}^{1} \nsubseteq \mathring{R}^{01}$ or $R_{42}^{2} \nsubseteq \mathring{R}^{02}$). In Figure 5.4, it can be observed that $R_{42}^{1} \nsubseteq \breve{R}_{42}^{11}$ and $R_{42}^{2} \subseteq \breve{R}_{42}^{22}$ hold, which means that the second sensor fault has occurred by the transient-state FI strategy. Moreover, if considering the steady-state FI strategy in Proposition 5.3, one can observe that $\mathbf{0} \notin R_{47}^{1}$ (or/and $\mathbf{0} \in R_{47}^{2}$) holds, which is in accordance with Row 2 of the matrix $\mathcal{I}'$ in (5.41), which means that at time instant 47, the fault can also be isolated by the steady-state FI strategy.

Remark 5.22. *According to the proposed FI algorithm, after a fault is detected, the fault should be either in the first or second sensor. Thus, as seen in the matrix $\mathcal{I}'$ in* (5.41)*, one only needs to use the residual zonotopes estimated by either the interval observer* 1 *or* 2 *(or both of these two interval observers), which corresponds to the bold and italic columns of Row* 1 *and* 2 *of the matrix $\mathcal{I}'$, respectively. This can reduce computational complexity of FI. Besides, because of space limit, please zoom in if some figures are not clear enough.*

5.7 Summary

This chapter proposes a sensor FDI approach based on set-theoretic approaches. In this approach, two different set-theoretic FDI mechanisms are simultaneously used, i.e., invariant set-based and interval observer-based mechanisms. This approach implements the combination of invariant sets and interval observers for sensor FDI, and both FD and FI decisions are based on these two FDI mechanisms. In order to reduce computational complexity, the available but redundant/unnecessary system-operating information is discarded by the proposed approach. For sensor faults, this approach can isolate faults during the transition induced by faults and the fastest FI case is that sensor faults are isolated at the same time when they are detected. For simplicity, this chapter only considers the linear time-invariant system with given magnitudes of sensor faults. However, in principle, it should be able to be extended to the system with parametric uncertainties and unknown but bounded sensor faults.

Part III

Fault-tolerant Control

Chapter 6

Fault-tolerant Model Predictive Control for Actuator Faults

This chapter focuses on the implementation of an actuator FTMPC scheme. In this FTMPC scheme, tube-MPC is used as the control strategy, FD is implemented by invariant sets and FI is done by MPC and tubes. Different from the passive fault diagnosis approaches proposed in the previous part, this chapter proposes an active FI method by using the constraint-handling ability of MPC, which can reduce the conservatism of guaranteed FI conditions. At the end of this chapter, an example is used to illustrate the effectiveness of the proposed FTMPC scheme.

6.1 Introduction

In the previous part, one proposed the actuator and sensor FDI approaches. However, since the proposed methods are passive, where only the process information captured by interval observers can be used for FDI, one can only reduce the conservatism by making full use of those obtained system-operating information.

Obviously, this passive acquisition of the system-operating information always has a bottleneck. In this part, one proposes an active approach to break through the mentioned bottleneck of the passive methods by using the constraint-handling ability of MPC. This active approach can obtain less conservative FI conditions by manipulating control inputs to excite the system. In this case, one can obtain more fault information that is unobtainable only by means of the passive methods.

Considering that MPC can explicitly deal with multivariable constrained systems, it is meaningful to implement MPC schemes with fault-tolerant capability. Actually, the FTMPC technique has been investigated in the literature, which is presented in Part I. Comparing with the FTMPC schemes proposed in [51, 71], this chapter proposes a

new FTMPC scheme, which cannot only obtain FI guarantees with less conservative FI conditions but also implement FTC with low computational complexity.

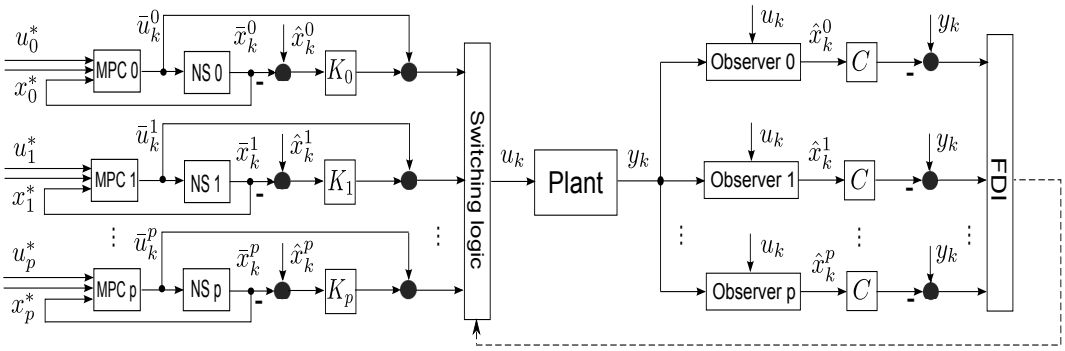


Figure 6.1: Actuator FTMPC scheme

For less complexity, one selects tube-based MPC as the control strategy in this proposed FTMPC scheme. Instead of interval observers, one only uses Luenberger observers, which cannot only reduce computational complexity but also accord with the tube-based MPC framework based on Luenberger observers. Additionally, considering different characteristics of actuator and sensor faults, this chapter only concentrates on coping with tolerance of actuator faults. The proposed FTMPC scheme is shown in Figure 6.1.

6.2 Problem Formulation

6.2.1 Plant Models

In this chapter, one considers the linear discrete time-invariant plant under the effect of actuator faults, which is modelled as (4.1). As the objective of this chapter is to propose an actuator FTC scheme, one should make several assumptions as in the previous part.

Assumption 6.1. *The pairs (A, BF_i) for all $i \in \mathbb{I}$ and (A, C) are stabilizable and detectable, respectively.*

Assumption 6.2. *The occurrence of actuator mode can persist sufficiently long time such that the FDI module has enough responsive time to detect and isolate them.*

Remark 6.1. *For simplicity, this chapter only considers single faults but the proposed approach can also be extended for the case of multiple faults in principle.*

In Chapter 4, the proposed actuator FDI approach considers unknown but bounded faults, which accords with the realistic fault features that fault magnitudes are generally unknown. But, for simplicity, this chapter only considers faults with given magnitudes.

However, in principle, the proposed actuator FTC scheme should also be able to be extended for unknown but bounded actuator faults.

As said in Remark 6.1, the fault-modelling matrix F_i should take $p+1$ values ($i \in \mathbb{I} = \{0, 1, 2, \ldots, p\}$). In this chapter, for simplicity, one considers the complete actuator outage. Thus, F_0 is the identity matrix denoting the healthy actuator mode and F_i ($i \neq 0$) modelling the i-th actuator-fault mode is expressed as

$$F_i = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & \overset{i}{\downarrow}\ 0 & \\ & & & \ddots \\ & & & & 1 \end{bmatrix}. \tag{6.1}$$

Additionally, the hard state and input constraints are considered, which are denoted as

$$X = \{x \in \mathbb{R}^n : |x - x^c| \leq \bar{x}, x^c \in \mathbb{R}^n, \bar{x} \in \mathbb{R}^n\}, \tag{6.2a}$$
$$U = \{u \in \mathbb{R}^p : |u - u^c| \leq \bar{u}, u^c \in \mathbb{R}^p, \bar{u} \in \mathbb{R}^p\}, \tag{6.2b}$$

respectively, where all the vectors x^c, u^c, $\bar{x}$ and $\bar{u}$ are constant and known.

6.2.2 Setpoint Tracking

There are totally $p+1$ considered actuator modes (healthy or faulty), for each mode, one has an output-tracking objective. Hence, one should have $p+1$ reference models, each of which corresponds to one considered actuator mode. For the i-th actuator mode, the corresponding reference model is given as

$$x_{k+1}^{ref} = Ax_k^{ref} + BF_i u_k^{ref}, \tag{6.3a}$$
$$y_k^{ref} = Cx_k^{ref}, \tag{6.3b}$$

where u_k^{ref}, x_k^{ref} and y_k^{ref} denote the reference inputs, states and outputs, respectively.

Remark 6.2. *In this chapter, without loss of generality, one considers tracking given output setpoints. The same principle could be extended to deal with time-variant reference-tracking problem. Besides, if necessary, one can also add the vectors ω^c and η^c into the reference model (6.3).*

In the i-th actuator mode, the control objective is to track a given setpoint y_i^*, i.e., in the absence of uncertainties and/or faults, one should have

$$\lim_{k\to\infty} (y_k - y_i^*) \to 0. \tag{6.4}$$

By using (6.3), a state-input setpoint pair (x_i^*,u_i^*) in the steady-state operation of the i-th actuator mode can be computed by

$$\begin{bmatrix} A - I & BF_i \\ C & O \end{bmatrix} \begin{bmatrix} x_i^* \\ u_i^* \end{bmatrix} = \begin{bmatrix} O \\ y_i^* \end{bmatrix}. \tag{6.5}$$

Assumption 6.3. *The equation* (6.5) *for all* $i \in \mathbb{I}$ *is solvable in order to obtain the corresponding state-input setpoint pair.*

It can be observed that, under Assumption 6.3, a state-input setpoint pair (x_i^*, u_i^*) corresponding to y_i^* can be obtained by solving (6.5). Note that, for each mode, the state-input setpoint pair may be not unique.

Remark 6.3. *Ideally, the system control objective should be able to track a given output signal, i.e., all the* $p + 1$ *given outputs should be the same. But, under the effect of faults, sometimes, the closed-loop system has to face a degree of performance degradation. In this case, the given output setpoints may take different values.*

6.2.3 Observers

A bank of observers are designed for the proposed actuator scheme, each of which is designed to match one actuator mode. Thus, the observer matching the j-th ($j \in \mathbb{I}$) mode can be designed as

$$\hat{x}_{k+1}^j = (A - L_j C)\hat{x}_k^j + BF_j u_k + L_j y_k, \tag{6.6a}$$

$$\hat{y}_k^j = C\hat{x}_k^j, \tag{6.6b}$$

where $\hat{x}_k^j$ and $\hat{y}_k^j$ are the estimated states and outputs, respectively, and L_j is the j-th observer gain.

Assumption 6.4. *For each observer, the corresponding observer gain can stabilize the observer dynamics, i.e., for all* $j \in \mathbb{I}$, $A - L_j C$ *is a Schur matrix.*

Note that, under Assumption 6.1, it is always possible to find a gain matrix L_j that satisfies Assumption 6.4.

6.2.4 Model Predictive Controllers

For the collection of the considered actuator modes, a bank of tube-based MPC controllers are used to control the system, each of which corresponds to one actuator mode. As introduced in Chapter 2, the nominal system corresponding to the i-th actuator mode is obtained by neglecting the uncertainties ω_k and η_k, which is given as

$$\bar{x}_{k+1}^i = A\bar{x}_k^i + BF_i\bar{u}_k^i, \tag{6.7a}$$

$$\bar{y}_k^i = C\bar{x}_k^i. \tag{6.7b}$$

Remark 6.4. *Similar with Remark 6.2, if necessary, the vectors* ω^c *and* η^c *can be added into the nominal system* (6.7).

According to [35], the control law of the i-th tube-based MPC controller has the following form

$$u_k = \bar{u}_k^i + K_i(\hat{x}_k^i - \bar{x}_k^i), \tag{6.8}$$

where $\bar{u}_k^i$ is generated by the nominal optimization problem of the i-th tube-based MPC controller (see (2.14)). The i-th nominal optimization problem uses (6.7) as its internal model and K_i is the feedback gain designed for the i-th tube-based MPC controller.

6.3 Fault Detection and Isolation

6.3.1 System Analysis

In the steady-state operation of the i-th actuator mode, the i-th tube-based MPC controller, the i-th state-input pair (x_i^*, u_i^*) and the i-th observer are used in the closed-loop system. The state estimation error of the j-th observer in the i-th mode is defined as

$$\tilde{x}_k^{i,j,i} = x_k - \hat{x}_k^j. \tag{6.9}$$

Remark 6.5. *In the superscript of $\tilde{x}_k^{i,j,i}$, the first index denotes that the plant is in the i-th mode, the second index denotes the j-th observer and the third index denotes that the i-th tube-based MPC controller is active in the closed-loop system.*

In (6.9), if $j \neq i$, using (4.1), (6.6) and (6.8), the dynamics of $\tilde{x}_k^{i,j,i}$ are derived as

$$\tilde{x}_{k+1}^{i,j,i} = (A - L_jC)\tilde{x}_k^{i,j,i} + B(F_i - F_j)\bar{u}_k^i + B(F_i - F_j)K_i(\hat{x}_k^i - \bar{x}_k^i) + \omega_k - L_j\eta_k \tag{6.10}$$

and the corresponding output estimation error of the j-th observer is derived as

$$\begin{aligned} \tilde{y}_k^{i,j,i} &= y_k - \hat{y}_k^j \\ &= C\tilde{x}_k^{i,j,i} + \eta_k. \end{aligned} \tag{6.11}$$

Besides, in the steady-state operation of the i-th mode, the term $\hat{x}_k^i - \bar{x}_k^i$ occurring in (6.8) and (6.10) is denoted by

$$e_k^{i,i,i} = \hat{x}_k^i - \bar{x}_k^i, \tag{6.12}$$

whose dynamics can be derived by using (6.6) and (6.7) as

$$e_{k+1}^{i,i,i} = (A + BF_iK_i)e_k^{i,i,i} + L_iC\tilde{x}_k^{i,i,i} + L_i\eta_k, \tag{6.13}$$

where $\tilde{x}_k^{i,i,i}$ corresponds to the case of $j = i$ in (6.9) and its dynamics can be obtained by letting $j = i$ in (6.10), i.e.,

$$\tilde{x}_{k+1}^{i,i,i} = (A - L_iC)\tilde{x}_k^{i,i,i} + \begin{bmatrix} I & -L_i \end{bmatrix} \begin{bmatrix} \omega_k \\ \eta_k \end{bmatrix}. \tag{6.14}$$

Assumption 6.5. *The matrix $A + BF_iK_i$ for all $i \in \mathbb{I}$ is a Schur matrix.*

Since $\omega_k \in W$ and $\eta_k \in V$ are bounded as defined in (3.2), an RPI set (denoted as $\tilde{X}^{i,i,i}$) of $\tilde{x}_k^{i,i,i}$ can be constructed. According to the notion of invariant sets, as long as $\tilde{x}_{k^*}^{i,i,i} \in \tilde{X}^{i,i,i}$, $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$ always holds for all $k > k^*$. Similarly, considering $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$, an RPI set (denoted as $E^{i,i,i}$) of $e_k^{i,i,i}$ can be constructed by using (6.13).

In the i-th mode, if a fault is detected, for the FI point of view, one defines an input set $\bar{U}_f^i$ for the nominal control input $\bar{u}_k^i$ (i.e., $\bar{u}_k^i \in \bar{U}_f^i$) as

$$\bar{U}_f^i = \{\bar{u}^i \in \mathbb{R}^p : \left|\bar{u}^i - \bar{u}_f^{i,c}\right| \leq \bar{u}_f^i, \bar{u}_f^{i,c} \in \mathbb{R}^p, \bar{u}_f^i \in \mathbb{R}^p\},$$

where the vectors $\bar{u}_f^{i,c}$ and $\bar{u}_f^i$ are constant and known.

Remark 6.6. *The input set $\bar{U}_f^i$ is only used for on-line FI when a fault is detected in the i-th actuator mode. The use of $\bar{U}_f^i$ will be detailed in the following contents.*

Similarly, if considering $e_k^{i,i,i} \in E^{i,i,i}$ and $\bar{u}_k^i \in \bar{U}_f^i$ in (6.10), an RPI set (denoted as $\tilde{X}^{i,j,i}$) of $\tilde{x}_k^{i,j,i}$ can be obtained. The corresponding set of the output estimation error is

$$\tilde{Y}^{i,j,i} = C\tilde{X}^{i,j,i} \oplus V, \tag{6.15}$$

where, in the case of $j = i$, the output estimation error set $\tilde{Y}^{i,i,i}$ corresponding to $\tilde{X}^{i,i,i}$ can be obtained as well.

Remark 6.7. *From the FD point of view, all the RPI sets $\tilde{X}^{i,i,i}$, $E^{i,i,i}$ and $\tilde{X}^{i,j,i}$ should be as small as possible.*

Since $\tilde{y}_k^{i,j,i}$ is available while $\tilde{x}_k^{i,j,i}$ is unavailable, $\tilde{y}_k^{i,j,i}$ is used as the residual signal in this proposed FTC scheme.

6.3.2 Fault Detection

The FD approach used in this scheme is a passive approach, which is based on invariant sets. Thus, the FD task can be simplified into only testing whether the residual $\tilde{y}_k^{i,j,i}$ is inside its corresponding set or not. The advantage of the invariant set-based FD consists in its low complexity.

As analyzed in Subsection 6.3.1, for each mode $i \in \mathbb{I}$, only the sets $\tilde{X}^{i,i,i}$ and $\tilde{Y}^{i,i,i}$ are independent of $\bar{u}_k^i$, while $\tilde{X}^{i,j,i}$ and $\tilde{Y}^{i,j,i}$ ($j \neq i$) depend on $\bar{u}_k^i$. Thus, in order to assure that FD is not affected by the FI task (the FI details will be given in next sections), in the i-th mode, only the set $\tilde{Y}^{i,i,i}$ is used for the FD task, i.e., testing whether or not

$$\tilde{y}_k^{i,i,i} \in \tilde{Y}^{i,i,i} \tag{6.16}$$

is violated in real time. If a violation of (6.16) is detected, it means that a fault has occurred. Otherwise, it is considered that the system still operates in the i-th mode.

Note that, for some faults, even though they occur in the system, perhaps (6.16) is still not violated. This means that these faults cannot be detected, isolated and actively tolerated by the proposed scheme. Instead, they can only be implicitly tolerated to some extent by the PFTC ability of the proposed scheme.

6.3.3 Fault Isolation

6.3.3.1 System after Actuator Faults

The FI task is started when a fault is detected. Without loss of generality, it is assumed that the l-th fault occurs at time instant k_d. Although the mode has changed from i to l, before the fault is isolated (i.e., the system is reconfigured), the system structure does not change yet, which implies that the closed-loop system is still composed of the same components.

As per (4.1), (6.6), (6.7) and (6.8), when the l-th fault occurs, the state estimation error of the j-th observer changes from $\tilde{x}_k^{i,j,i}$ to $\tilde{x}_k^{l,j,i}$ with the dynamics

$$\tilde{x}_{k+1}^{l,j,i} = (A - L_jC)\tilde{x}_k^{l,j,i} + B(F_l - F_j)\bar{u}_k^i + B(F_l - F_j)K_i e_k^{l,i,i} + \omega_k - L_j\eta_k \tag{6.17}$$

and $e_k^{i,i,i}$ in (6.13) changes to $e_k^{l,i,i}$ with the dynamics

$$e_{k+1}^{l,i,i} = (A + BF_iK_i)e_k^{l,i,i} + L_iC\tilde{x}_k^{l,i,i} + L_i\eta_k. \tag{6.18}$$

In order to collect the whole process information after the l-th fault from the i-th mode, one defines a vector

$$\xi_k^{i\to l} = \begin{bmatrix} \tilde{x}_k^{l,0,i} \\ \vdots \\ \tilde{x}_k^{l,i,i} \\ \vdots \\ \tilde{x}_k^{l,p,i} \\ e_k^{l,i,i} \end{bmatrix}.$$

As per (6.17) and (6.18), the dynamics of $\xi_k^{i\to l}$ can be obtained as

$$\xi_{k+1}^{i\to l} = A_{i\to l}\xi_k^{i\to l} + B_{i\to l}\bar{u}_k^i + E_{i\to l}^{\omega}\omega_k + E_{i\to l}^{\eta}\eta_k, \tag{6.19}$$

where

$$A_{i\to l} = \begin{bmatrix} A-L_0C & O & \cdots & O & B(F_l-F_0)K_i \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ O & A-L_iC & \cdots & O & B(F_l-F_i)K_i \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ O & O & \cdots & A-L_pC & B(F_l-F_p)K_i \\ O & L_iC & \cdots & O & A+BF_iK_i \end{bmatrix},$$

$$B_{i\to l} = \begin{bmatrix} B(F_l - F_0) \\ \vdots \\ B(F_l - F_i) \\ \vdots \\ B(F_l - F_p) \\ O \end{bmatrix}, E^{\omega}_{i\to l} = \begin{bmatrix} I \\ \vdots \\ I \\ \vdots \\ I \\ O \end{bmatrix}, E^{\eta}_{i\to l} = \begin{bmatrix} -L_0 \\ \vdots \\ -L_i \\ \vdots \\ -L_p \\ L_i \end{bmatrix}.$$

Assumption 6.6. *For the i-th mode, the observer and feedback gains $L_0, L_1, \ldots, L_p$ and K_i can assure that the matrix $A_{i\to l}$ is a Schur. Moreover, for the other considered modes, this condition should also be satisfied.*

Similarly, considering $\bar{u}^i_k \in \bar{U}^i_f$, $\omega_k \in W$ and $\eta_k \in V$, an RPI set of $\xi^{i\to l}_k$ can be computed, which is denoted as $\Xi^{i\to l}$. By projecting $\Xi^{i\to l}$ towards the component space, an RPI set of each component of $\xi^{i\to l}_k$ can be obtained. For example, an RPI set (denoted as $\tilde{X}^{l,j,i}$) of $\tilde{x}^{l,j,i}_k$ can be obtained by projecting $\Xi^{i\to l}$ to the space of $\tilde{x}^{l,j,i}_k$. Similarly, an RPI set (denoted as $E^{l,i,i}$) of $e^{l,i,i}_k$ can be computed by projection. This implies that, after the l-th fault, $\tilde{x}^{l,j,i}_k$ and $e^{l,i,i}_k$ should enter into $\tilde{X}^{l,j,i}$ and $E^{l,i,i}$, respectively. Moreover, the set of the output estimation error corresponding to $\tilde{X}^{l,j,i}$ is

$$\tilde{Y}^{l,j,i} = C\tilde{X}^{l,j,i} \oplus V. \tag{6.20}$$

Thus, the sets of output estimation errors corresponding to each observer and each mode (the i-th mode or a mode switching from the i-th mode) are listed in Table 6.1, where each row corresponds to one actuator mode.

Table 6.1: Sets of output estimation errors

	Observer 0	$\cdots$	Observer i	$\cdots$	Observer p
Mode 0	$\tilde{Y}^{0,0,i}$	$\cdots$	$\tilde{Y}^{0,i,i}$	$\cdots$	$\tilde{Y}^{0,p,i}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode i	$\tilde{Y}^{i,0,i}$	$\cdots$	$\tilde{Y}^{i,i,i}$	$\cdots$	$\tilde{Y}^{i,p,i}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode p	$\tilde{Y}^{p,0,i}$	$\cdots$	$\tilde{Y}^{p,i,i}$	$\cdots$	$\tilde{Y}^{p,p,i}$

6.3.3.2 Residual Tubes

The dynamics of $\tilde{x}^{l,l,i}$ extracted from (6.19) is used for FI, which has the form

$$\tilde{x}^{l,l,i}_{k+1} = (A - L_l C)\tilde{x}^{l,l,i}_k + \omega_k - L_l\eta_k. \tag{6.21}$$

Substituting W and V into (6.21), the set-based descriptions of $\tilde{x}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i}$ can be obtained as

$$\tilde{X}_{k+1}^{l,l,i} = (A - L_l C)\tilde{X}_k^{l,l,i} \oplus W \oplus (-L_l V), \tag{6.22a}$$

$$\tilde{Y}_k^{l,l,i} = C\tilde{X}_k^{l,l,i} \oplus V. \tag{6.22b}$$

Proposition 6.1. *Given that the l-th ($l \neq i$) fault has occurred in the i-th mode and the state estimation error of the l-th observer is bounded by a set $\tilde{X}_{k*}^{l,l,i}$ at time instant $k*$, if $\tilde{X}_{k*}^{l,l,i}$ is used to initialize (6.22) to generate tubes, $\tilde{x}_k^{l,l,i} \in \tilde{X}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i} \in \tilde{Y}_k^{l,l,i}$ will hold for all $k \geq k*$.*

Proof : Since (6.22a) considers the worst case of uncertainties in (6.21), if at time instant $k*$, $\tilde{x}_{k*}^{l,l,i} \in \tilde{X}_{k*}^{l,l,i}$ holds, it implies that $\tilde{x}_k^{l,l,i} \in \tilde{X}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i} \in \tilde{Y}_k^{l,l,i}$ will always hold for all $k \geq k*$. □

In the i-th mode, it is assumed that the l-th fault is detected at time instant k_d. If an initial set is used to initialize (6.22a) at time instant k_d, the set tubes of state and output estimation errors generated by (6.22) are denoted as

$$\tilde{\mathbb{T}}_{k_d}^{x,l,l,i} = \{\tilde{X}_{k_d}^{l,l,i}, \tilde{X}_{k_d+1}^{l,l,i}, \tilde{X}_{k_d+2}^{l,l,i}, \dots\}, \tag{6.23a}$$

$$\tilde{\mathbb{T}}_{k_d}^{y,l,l,i} = \{\tilde{Y}_{k_d}^{l,l,i}, \tilde{Y}_{k_d+1}^{l,l,i}, \tilde{Y}_{k_d+2}^{l,l,i}, \dots\}. \tag{6.23b}$$

Remark 6.8. *Generally, when the system is in the i-th mode, the detection of a violation of (6.16) implies that a mode switching from i to another unknown mode denoted as f ($f \in \mathbb{I}_i$) has occurred. Thus, for FI, one has to obtain all the p output estimation error set tubes $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$ ($l \in \mathbb{I}_i$).*

Thus, at time instant k_d, the proposed FI algorithm generates p output-estimation-error set tubes $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$ ($l \in \mathbb{I}_i$), each of which corresponds to a candidate actuator mode. Moreover, for the p corresponding observers, as long as

$$\tilde{x}_{k_d}^{f,l,i} \in \tilde{X}_{k_d}^{l,l,i},\ f,\ l \in \mathbb{I}_i \tag{6.24}$$

is guaranteed at time instant k_d such that

$$\tilde{y}_{k_d}^{f,l,i} \in \tilde{Y}_{k_d}^{l,l,i},$$

it implies that, among the p output-estimation-error set tubes $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$, there exists at least one set tube (assume that it is indexed by m) that can always satisfy

$$\tilde{y}_k^{f,m,i} \in \tilde{Y}_k^{m,m,i},\ k \geq k_d,\ f,\ m \in \mathbb{I}_i. \tag{6.25}$$

Remark 6.9. *As per Proposition 6.1, if the fault is the l-th one ($f = l$) and (6.24) holds at time instant k_d, for all $k \geq k_d$, $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$ can always satisfy $\tilde{y}_k^{f,l,i} \in \tilde{Y}_k^{l,l,i}$.*

Remark 6.9 implies that the fault will be indicated by one of the output tubes, which can always satisfy (6.25).

6.3.3.3 Fault Isolation Algorithm

In order to isolate a fault, one has to guarantee that one and only one tube can always satisfy its corresponding inclusion (6.25) after FD and then the fault can be indicated by the index of this tube. Based on this idea, one establishes guaranteed FI conditions as presented in Proposition 6.2.

Proposition 6.2. *When the system is in the i-th actuator mode, for any observer (assume that it is indexed by j), if all the $p+1$ output-estimation-error sets corresponding to this observer (i.e., the $p+1$ sets in the j-th column of Table 6.1) satisfy*

$$\tilde{Y}^{j,j,i} \cap \bigcup_{l=0}^{p} \tilde{Y}^{l,j,i} = \varnothing,\ j \neq i,\ l \neq i,\ l \neq j,\ i,\ j,\ l \in \mathbb{I}, \tag{6.26}$$

once a mode switching from the i-th mode to another considered mode is detected at time instant k_d, this mode can be isolated during the transition by searching the output-estimation-error tube that can always satisfy (6.25) for all $k \geq k_d$.

Proof : The tube $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ will finally enter into $\tilde{Y}^{j,j,i}$ and stay inside. If (6.26) holds, the tube $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ can persistently confine the output estimation error $\tilde{y}_k^{l,j,i}$ only under the condition $l = j$. If $l \neq j$, at the first several steps, $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ is able to confine $\tilde{y}_k^{l,j,i}$ because of the initialization condition (6.24). But, as $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ approaches $\tilde{Y}^{j,j,i}$, $\tilde{y}_k^{l,j,i}$ must diverge from $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$. This implies that, under the condition (6.26), by searching the tube that is always able to confine $\tilde{y}_k^{l,j,i}$ after FD, the fault can be isolated. □

6.3.3.4 Construction of Starting Sets

According to the aforementioned FI principle, it is known that the key of this proposed FI approach consists in constructing starting sets that satisfy (6.24) at time instant k_d to initialize (6.22) to generate the output-estimation-error tubes. Here, one takes the j-th observer as an example to show the method of constructing starting sets. Thus, according to (6.11), one can obtain

$$C\tilde{x}_{k_d}^{i,j,i} \in \{\tilde{y}_{k_d}^{i,j,i}\} \oplus (-V). \tag{6.27}$$

With (6.27), a set to bound $\tilde{x}_{k_d}^{i,j,i}$ can always be constructed to initialize (6.22a) to generate the output-estimation-error tubes. Either of the two methods in Properties 2.4 and 2.5 can use (6.27) to construct starting zonotopic sets to contain $\tilde{x}_{k_d}^{i,j,i}$. The details on these two methods are omitted here.

Remark 6.10. *If the matrix C is invertible, a set to bound $\tilde{x}_{k_d}^{i,j,i}$ can be directly obtained by (6.27) with the inverse of C.*

Moreover, it can be observed that, for the j-th observer, the expression of (6.27) is independent of system mode switching. This means that (6.27) can always be used to construct a set to bound state estimation errors of the j-th observer in any mode.

Remark 6.11. *Since X, U, W and V can be rewritten as zonotopes, from the computational point of view, all the tubes are generated by using zonotopes in this chapter. Thus, the starting sets are also constructed as zonotopes.*

6.4 Fault-tolerant Control

As aforementioned, tube-based MPC is used in the proposed actuator FTC scheme. The important advantages of the tube-based MPC are that it can effectively deal with system constraints and has relatively low computational complexity.

6.4.1 Model Predictive Control

The tube-based MPC technique proposed in [35] is adopted to implement FTC in this scheme. Hence, please see [35] for more details. Among a bank of tube-based MPC controllers, the control law of the i-th one is given in (6.8). Firstly, it is assumed that the closed-loop system is in the steady-state operation of the i-th mode. The key part of the i-th tube-based MPC controller is the open-loop optimization problem included in the controller, which is based on the i-th nominal system.

In reality, it is known that X and U presented in (6.2) are the hard constraints of the system. Note that, these hard constraints imply the indirect constraints on the nominal system-based open-loop optimization problem. In the case of the i-th mode, the indirect input constraint is via (6.8), i.e., $u_k = \bar{u}_k^i + K_i e_k^{i,i,i}$. As per Section 6.3.1, in the steady-state operation, $e_k^{i,i,i} \in E^{i,i,i}$ holds, Thus, the input constraints of the i-th nominal system-based open-loop optimization problem can be obtained as

$$\bar{u}_k^i \in \bar{U}^i = U \ominus K_i E^{i,i,i}. \tag{6.28}$$

Considering $x_k = \bar{x}_k^i + e_k^{i,i,i} + \tilde{x}_k^{i,i,i}$ ($e_k^{i,i,i} \in E^{i,i,i}$ and $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$), the state constraints of the i-th nominal system-based open-loop optimization problem can be obtained as

$$\bar{x}_k^i \in \bar{X}^i = U \ominus (E^{i,i,i} \oplus \tilde{X}^{i,i,i}). \tag{6.29}$$

Assumption 6.7. *For all $i \in \mathbb{I}$, the constraint sets $\bar{X}^i$ and $\bar{U}^i$ are nonempty.*

Thus, the open-loop optimization problem of the i-th tube-based MPC controller,

based on the i-th nominal system in (6.7), has the following form

$$\begin{aligned} J_k = \min_{\bar{\mathbf{u}}^i} \sum_{j=0}^{N-1} \|(\bar{x}^i_{k+j|k} - x^*_i)\|^2_{Q_i} + \|(\bar{u}^i_{k+j|k} - u^*_i)\|^2_{R_i} + \|(\bar{x}^i_{k+N|k} - x^*_i)\|^2_{P_i} \\ \text{subject to} \quad \begin{aligned} \bar{x}^i_{k+j|k} &\in \bar{X}^i, \\ \bar{u}^i_{k+j|k} &\in \bar{U}^i, \\ \bar{x}^i_{k+N|k} &\in \bar{X}^i_T, \\ \bar{x}^i_{k|k} &= \bar{x}^i_k, \end{aligned} \end{aligned} \tag{6.30}$$

where N is the prediction horizon, $\bar{\mathbf{u}}^{\mathbf{i}} = [\bar{u}^i_{k|k}, \bar{u}^i_{k+1|k}, \ldots, \bar{u}^i_{k+N-1|k}]$ and Q_i, R_i and P_i are positive-definite matrices and $\bar{X}^i_T$ is the corresponding terminal state constraint set. If the terminal constraint set $\bar{X}^i_T$ is the MCI set of the i-th nominal system corresponding to the nominal constraint sets $\bar{X}^i$ and $\bar{U}^i$, the i-th tube-based MPC controller can be designed to be stable and recursively feasible. Moreover, under Assumptions 6.1 and 6.5, the tube-based MPC controller stabilizing the closed-loop systems can always be designed. Since the tube-based MPC technique used in this chapter is referred to [35], the relevant technical details are omitted here.

6.4.2 Transient-state Behaviors

Different from the steady-state operation of the i-th mode, once a fault has occurred (denoted by l), it implies that the system mode changes from i to l ($l \neq i$). In order to analyze the transient-state behaviors induced by a fault, one divides the transient-state process into two phases. The first phase starts from the occurrence of a fault till the detection of the fault and the second phase starts from the detection of the fault to the isolation of the fault. Since the second phase of the transition corresponds to the active FI phase in the FTC scheme, it will be discussed in the next subsection.

In the first phase of the transition, despite the l-th fault has occurred, the FD criterion (6.16), i.e., $\tilde{y}^{l,i,i}_k \in \tilde{Y}^{i,i,i}$, still holds. Since, before FI, one does not know the faulty system situation and the system is still composed of the same components with the i-th mode, although the l-th fault has occurred, during the first phase of the transition, one has to *think* that the system still operates in the i-th mode and can take no actions.

6.4.3 Active Fault Isolation

6.4.3.1 Fault Isolation Principle

Without considering the observer gains, feedback gains and faults, as per (6.19) and (6.20), when the system mode changes from i to l ($l \neq i$), the sets of output estimation errors are decided by those of uncertainties and nominal inputs. For simplicity of

understanding, one uses a function

$$\tilde{Y}^{l,j,i} = f^{i\to l}(\bar{U}_f^i, W, V),\ j \neq l, \tag{6.31}$$

to describe the relation between the sets of output estimation errors and those of uncertainties and nominal inputs, which implies that whether the FI conditions in Proposition 6.2 hold or not depends on the set of the nominal input $\bar{u}_k^i$. Note that, different from $Y^{l,j,i}$ ($j \neq l$), $Y^{l,l,i}$ is only decided by W and V and free from the effect of $\bar{U}_f^i$.

Assumption 6.8. *For all $i \in \mathbb{I}$, there exists a set $\bar{U}_f^i$ such that the FI conditions in Proposition 6.2 hold.*

Assumption 6.8 means that, when a switching from the mode i to l ($l \neq i$) is detected, since the FD time, if $\bar{u}_k^i$ is always confined inside $\bar{U}_f^i$, the FI conditions in Proposition 6.2 can be established on-line by the MPC controller and the proposed FI approach can isolate the mode. Thus, in the i-th mode, the i-th MPC controller has two different objectives:

- Steady-state operation (including the first-phase transition): no fault is detected and the task is to implement system performance. Thus, the input constraint of (6.30) is the set $\bar{U}^i$.
- Transient-state operation (only the second-phase transition): a fault is detected and the main task is to accurately isolate the fault and reconfigure the system. During this stage, the proposed FI approach actively switches the input constraint of (6.30) from $\bar{U}^i$ to $\bar{U}_f^i$ at the FD time k_d to establish the FI conditions on-line.

6.4.3.2 Transient-state Feasibility and Stability

The optimization problem (6.30) is updated by directly using the nominal state from the i-th nominal system. It is known that the nominal states are generated by the nominal system that is free from the effect of the real system. Thus, when the system is in the i-th mode, fault occurrence does not affect the feasibility and stability of the optimization problem (6.30) as long as the constraints X and U are not violated. However, the main concern is that fault occurrence may result in the violation of the system constraints X and U, which is key problem of the proposed approach.

During the FI process, since the input constraint of (6.30) is switched from $\bar{U}^i$ to $\bar{U}_f^i$ to establish the FI conditions on-line. In order to guarantee the feasibility and constraint satisfaction, one has to correspondingly switch the state and terminal state constraints of (6.30) from $\bar{X}^i$ to $\bar{X}_f^i$ and $\bar{X}_T^i$ to $\bar{X}_{fT}^{\ i}$, respectively. The set $\bar{X}_f^i$ is the state constraint set of (6.30) for the FI process and $\bar{X}_{fT}^{\ i}$ is a CI set of the i-th nominal system corresponding to $\bar{u}_k^i \in \bar{U}_f^i$ and $\bar{x}_k^i \in \bar{X}_f^i$. The sets $\bar{U}_f^i$ and $\bar{X}_f^i$ are a pair of design parameters to guarantee active FI in this FTC scheme.

Assumption 6.9. *For $i \in \mathbb{I}$, there exists a pair of input and state constraint sets $\bar{U}_f^i$ and $\bar{X}_f^i$ that can assure the constraints (6.2) are satisfied during active FI.*

Remark 6.12. *Before FI, one does not know which fault has occurred. However, since only a finite number of faults are considered in the scheme, a proper pair of $\bar{U}_f^i$ and $\bar{X}_f^i$ can be found by off-line simulations.*

In order to guarantee the feasibility of (6.30), one has to consider the nominal state $\bar{x}_{k_d}^i$ of the i-th nominal system at the FD time k_d.

Proposition 6.3. *At the FD time k_d, if $\bar{x}_{k_d}^i \in \bar{X}_{f_T}^{\ i}$ holds, (6.30) will be always feasible during the whole FI process.*

Proof : Since $\bar{X}_{f_T}^{\ i}$ is a CI set of the i-th nominal system under the input and state constraint sets $\bar{U}_f^i$ and $\bar{X}_f^i$, using $\bar{x}_k^i \in \bar{X}_{f_T}^{\ i}$ to update (6.30) implies $\bar{x}_{k+1}^i \in \bar{X}_{f_T}^{\ i}$ in terms of the definition of the CI sets. Thus, at time instant k_d, for all $k \geq k_d$, $\bar{x}_k^i \in \bar{X}_{f_T}^{\ i}$ can guarantee that there always exist control sequences such that the constraint $\bar{u}_k^i \in \bar{U}_f^i$ and $\bar{x}_k^i \in \bar{X}_f^i$ always hold during FI. □

In order to summarize, one proposes the following strategy to guarantee the feasibility of the MPC controller during FI:

- If $\bar{x}_{k_d}^i \in \bar{X}_{f_T}^{\ i}$, during FI, (6.30) is always feasible as per Proposition 6.3.
- If $\bar{x}_{k_d}^i \notin \bar{X}_{f_T}^{\ i}$, the center of $\bar{X}_{f_T}^{\ i}$ (constructed as a zonotope) is used to update (6.30) to guarantee feasibility at time instant k_d. For $k > k_d$, at one time instant $k*$, if $\bar{x}_{k^*}^i \in \bar{X}_{f_T}^{\ i}$, the feasibility of (6.30) can always be guaranteed for all $k > k^*$. Otherwise, continue to use the center of $\bar{X}_{f_T}^{\ i}$ to update (6.30).

Once a fault is isolated (denoted by l), the system will be reconfigured by using the l-th observer, the l-th state-input setpoint pair and the l-th tube-based MPC controller with the state, input and terminal constraint sets $\bar{X}^l$, $\bar{U}^l$ and $\bar{X}_T^l$. In this case, at the beginning of reconfiguration, one may also face the feasibility problem. In order to guarantee the feasibility during the initial stage after reconfiguration, the same principle with active FI to guarantee feasibility during FI can be used. As time elapses, the system gradually enters into the steady-state operation of the new mode and the new MPC controller will become feasible and the closed-loop system can operates normally again.

6.4.4 Fault-tolerant Control Algorithm

In order to summarize the FTC scheme proposed in this chapter, an FTMPC algorithm is presented in the following.

1. It is assumed that the system is in steady state of the i-th mode. The FD task consists in real-time testing whether (6.16) is violated or not. If (6.16) is not violated, it is considered that the system is still in the i-th mode. Otherwise, it implies that a fault has occurred.

2. Once a fault is detected at time instant k_d, the active FI approach is started to isolate the fault by respectively switching the constraints of (6.30) from $\bar{X}^i$, $\bar{U}^i$ and $\bar{X}^i_T$ to $\bar{X}^i_f$, $\bar{U}^i_f$ and $\bar{X}_{f_T}^{\ i}$ to satisfy the FI conditions on-line.

3. Simultaneously, at the FD time k_d, p output-estimation-error tubes (6.23) are initialized by the starting sets constructed by (6.27). For each tube, (6.25) is real-time tested. Whenever a tube violates (6.25), it is terminated and the index of this tube is removed from a collect of fault candidates. Until there is one and only one tube left, it implies that the fault is isolated.

4. Once the fault (assume that it is indexed by l) is isolated, the l-th observer, the l-th MPC controller and the l-th state-input setpoint pair are selected to reconfigure the system (the constraint sets are simultaneously switched to $\bar{X}^l$, $\bar{U}^l$ and $\bar{X}^l_T$ for the new MPC controller, respectively). Then, the whole procedure will be repeated to monitor this new mode again.

Remark 6.13. *Before, one discussed sensor FDI and FTC but did not mention system recovery from faulty to healthy. Actually, the proposed scheme can deal with system recovery with the same principle.*

6.5 Illustrative Example

In this section, an electric circuit from [41] is used as the case study of the proposed scheme, which is shown in Figure 6.2. The continuous-time dynamics of this circuit are given in [41], where the system matrices are

$$A = \begin{bmatrix} -\frac{1}{(R_1+R_2)C_p} & \frac{R_1}{(R_1+R_2)C_p} \\ \frac{1}{L}(\frac{R_2}{R_1+R_2}-1) & -\frac{1}{L}(\frac{R_1R_2}{R_1+R_2}-R_3) \end{bmatrix}, B = \begin{bmatrix} \frac{1}{(R_1+R_2)C_p} & 0 \\ -\frac{R_2}{L(R_1+R_2)} & \frac{1}{L} \end{bmatrix}, \tag{6.32a}$$

$$E = \begin{bmatrix} \frac{\alpha_1}{(R_1+R_2)C_p} \\ \frac{1}{L}(\alpha_2 - \frac{R_2}{R_1+R_2}\alpha_1) \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & R_3 \end{bmatrix}. \tag{6.32b}$$

All parameters of this circuit used here are from those in [41]. Please see [41] to obtain the definitions/values of all the signals/variables appearing in Figure 6.2. The only difference here is that one considers measurement noises in the current example. Note that the inputs of this circuit as shown in Figure 6.2 are the power sources $V_1(t)$ and $V_2(t)$, the states are composed of the capacitor voltage $v_C(t)$ and the inductor currency $i_L(t)$, the outputs are the voltages of the capacitor and the resistor R_3, and α_1

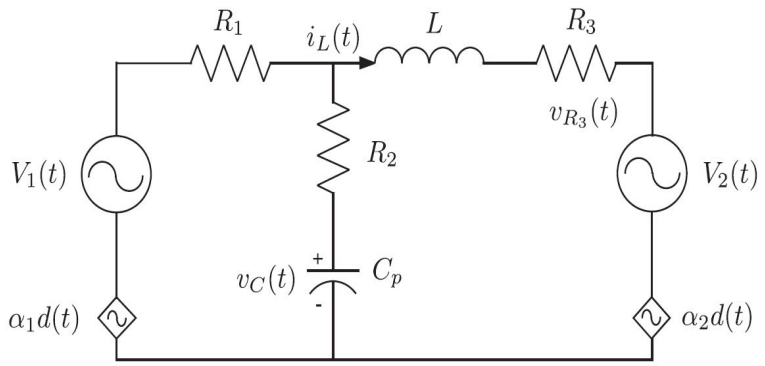


Figure 6.2: Circuit

and α_2 are proportionality constants. With a sampling time $1/15$s, the dynamics of the circuit can be discretized as

$$x_{k+1} = A_d x_k + B_d F_i u_k + E_d w_k, \tag{6.33a}$$
$$y_k = C_d x_k + \eta_k, \tag{6.33b}$$

with

$$A_d = \begin{bmatrix} 0.8693 & 2.6144 \\ -0.0016 & 1.0327 \end{bmatrix}, B_d = \begin{bmatrix} 0.131 & 0 \\ -0.082 & 0.083 \end{bmatrix}, E_d = \begin{bmatrix} 0.1307 \\ 0.0016 \end{bmatrix}, C_d = \begin{bmatrix} 1 & 0 \\ 0 & 20 \end{bmatrix}.$$

In (6.33), the uncertainties ω_k (originated from $d(t)$ in Figure 6.2) and η_k are bounded, whose bounds are given as $|\omega| \leq 1.5$ and $|\eta| \leq \begin{bmatrix} 0.05 & 0.05 \end{bmatrix}^T$. In this case study, two actuator faults are considered, either of which corresponds to one actuator. Thus, in total, there are three actuator modes considered, which are denoted as F_0 (healthy mode), F_1 (complete outage of the first actuator) and F_2 (complete outage of the second actuator). The values of these matrices are

$$F_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, F_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Additionally, the state and input constraints of the system are considered as

$$U = \{u : \begin{bmatrix} -10 \\ -10 \end{bmatrix} \leq u \leq \begin{bmatrix} 10 \\ 10 \end{bmatrix}\}, X = \{x : \begin{bmatrix} -10 \\ -10 \end{bmatrix} \leq x \leq \begin{bmatrix} 10 \\ 10 \end{bmatrix}\}.$$

Based on (6.33), three observers with the mathematical form (6.6) are designed, each of which matches one actuator mode. Correspondingly, three tube-based MPC controllers are designed to control the system, each of which is used for one mode.

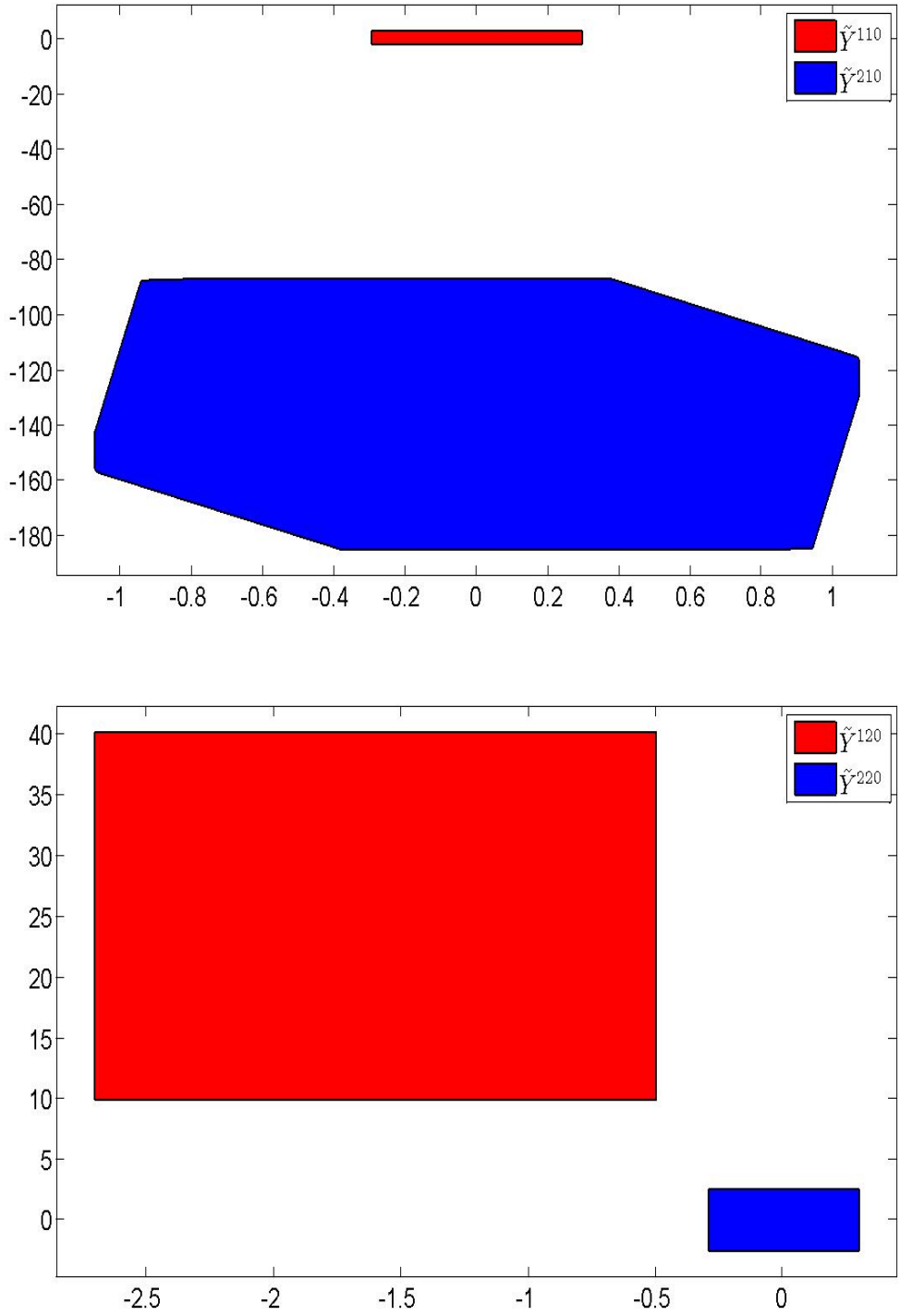


Figure 6.3: After-fault sets of output estimation errors

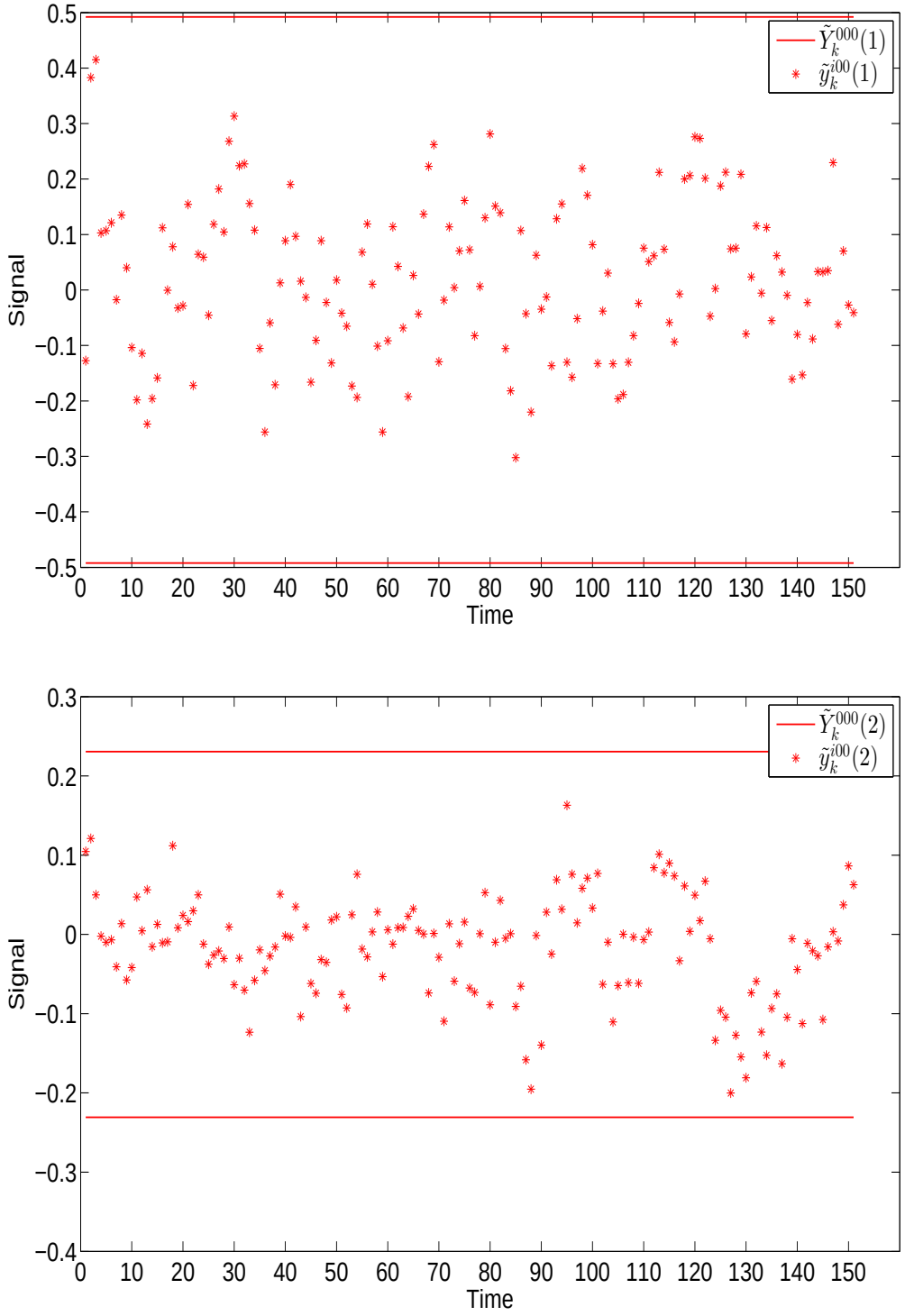


Figure 6.4: FD of Fault 1

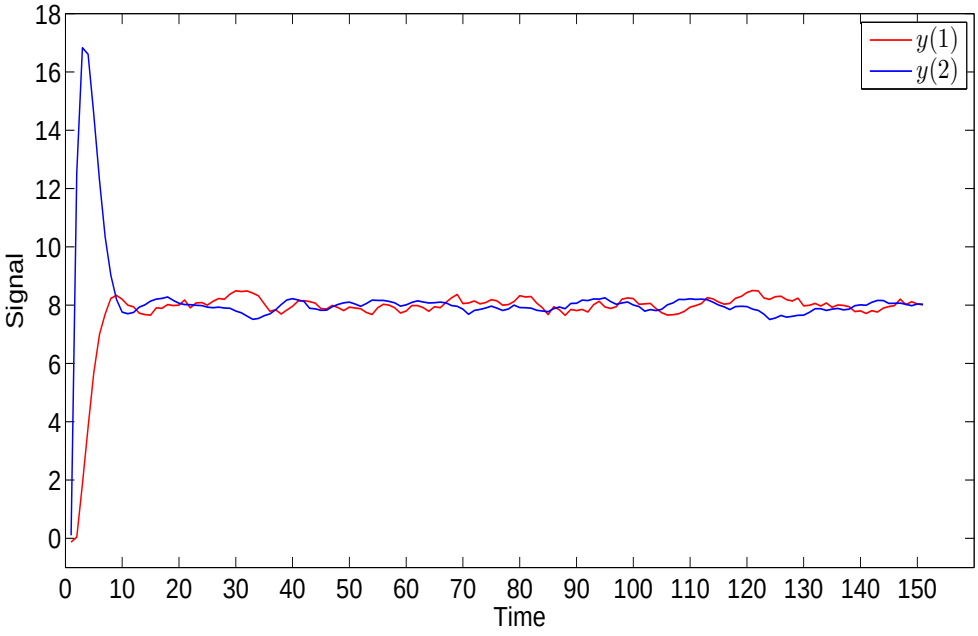


Figure 6.5: Outputs of Scenario 1

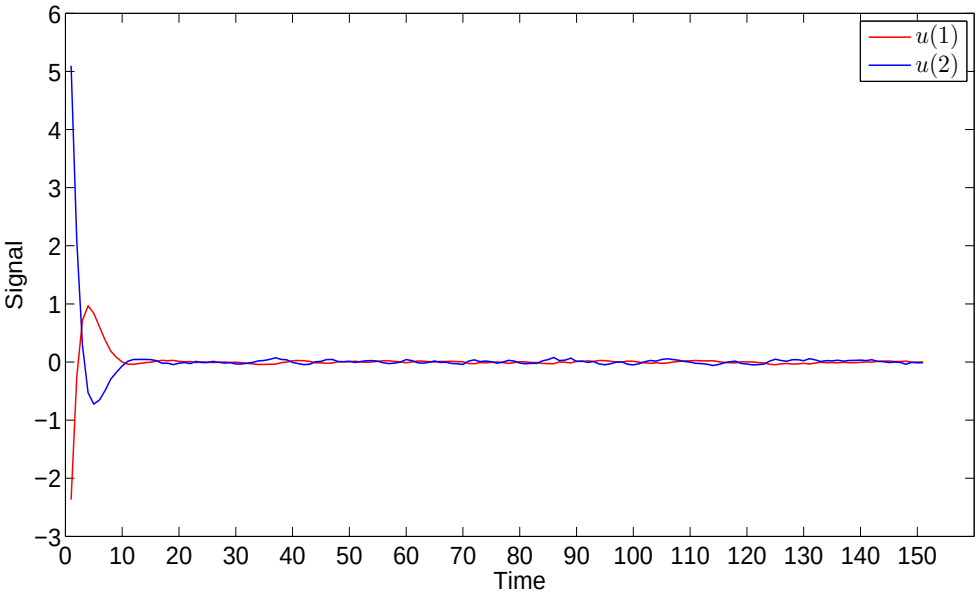


Figure 6.6: Inputs of Scenario 1

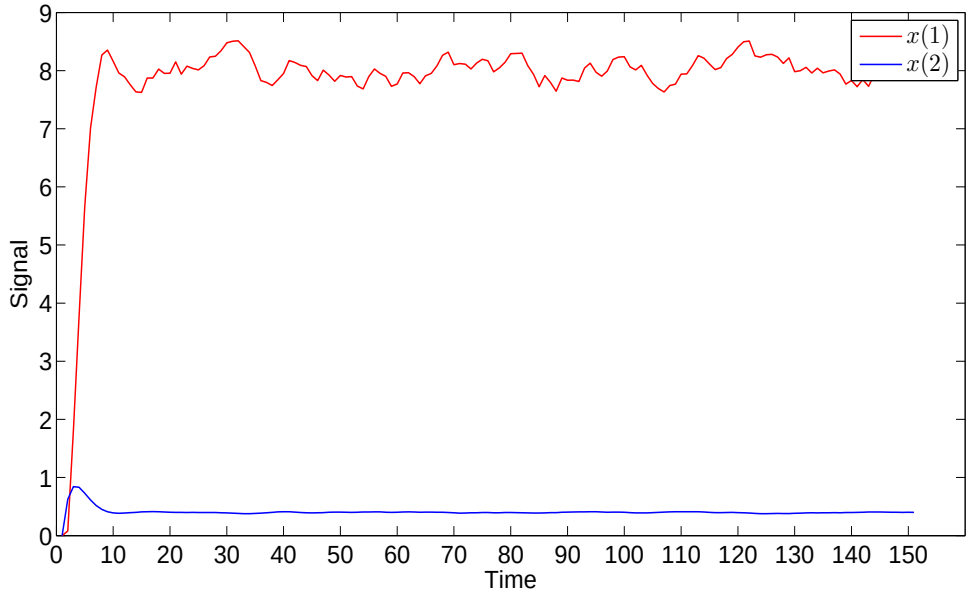


Figure 6.7: States of Scenario 1

Note that all the three tube-based MPC controllers should be designed to stabilize the closed-loop system. The corresponding feedback gains are designed as

$$K_0 = \begin{bmatrix} 0.1232 & 3.4734 \\ -0.3848 & -5.0688 \end{bmatrix}, K_1 = \begin{bmatrix} 0.1232 & 3.4734 \\ -0.3848 & -5.0688 \end{bmatrix}, K_2 = \begin{bmatrix} 0.1232 & 3.4734 \\ -0.3848 & -5.0688 \end{bmatrix}.$$

The output setpoints for the three actuator modes are respectively given as

$$y_0^* = \begin{bmatrix} 8 \\ 8 \end{bmatrix}, y_1^* = \begin{bmatrix} 5 \\ 5 \end{bmatrix}, y_2^* = \begin{bmatrix} 5 \\ 5 \end{bmatrix}.$$

Corresponding to these output setpoints, three state-input setpoint pairs can be obtained (each of which corresponds to one output setpoint)

$$x_0^* = \begin{bmatrix} 8.0 \\ 0.4 \end{bmatrix}, x_1^* = \begin{bmatrix} 5.0 \\ 0.25 \end{bmatrix}, x_2^* = \begin{bmatrix} 5.0 \\ 0.25 \end{bmatrix}, u_0^* = \begin{bmatrix} 0.888 \\ 0.178 \end{bmatrix}, u_1^* = \begin{bmatrix} 0 \\ 0.183 \end{bmatrix}, u_2^* = \begin{bmatrix} 0.178 & 0 \end{bmatrix}.$$

In this illustrative example, two fault scenarios are considered, each of which corresponds to one actuator fault:

- From time instants 0 to 75, the system is healthy and from time instants 76 to 150, the first actuator fault occurs.

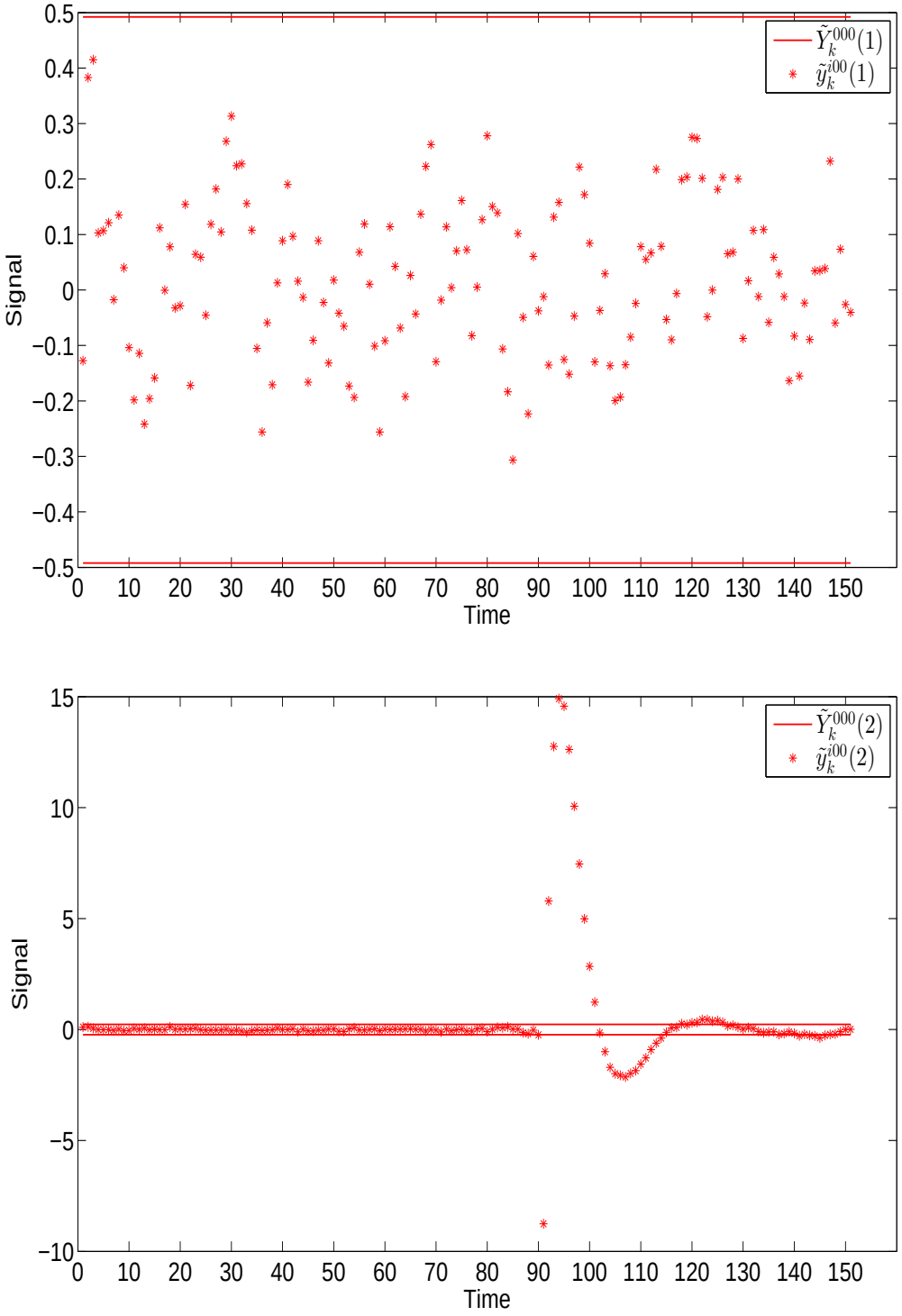


Figure 6.8: FD of Fault 2

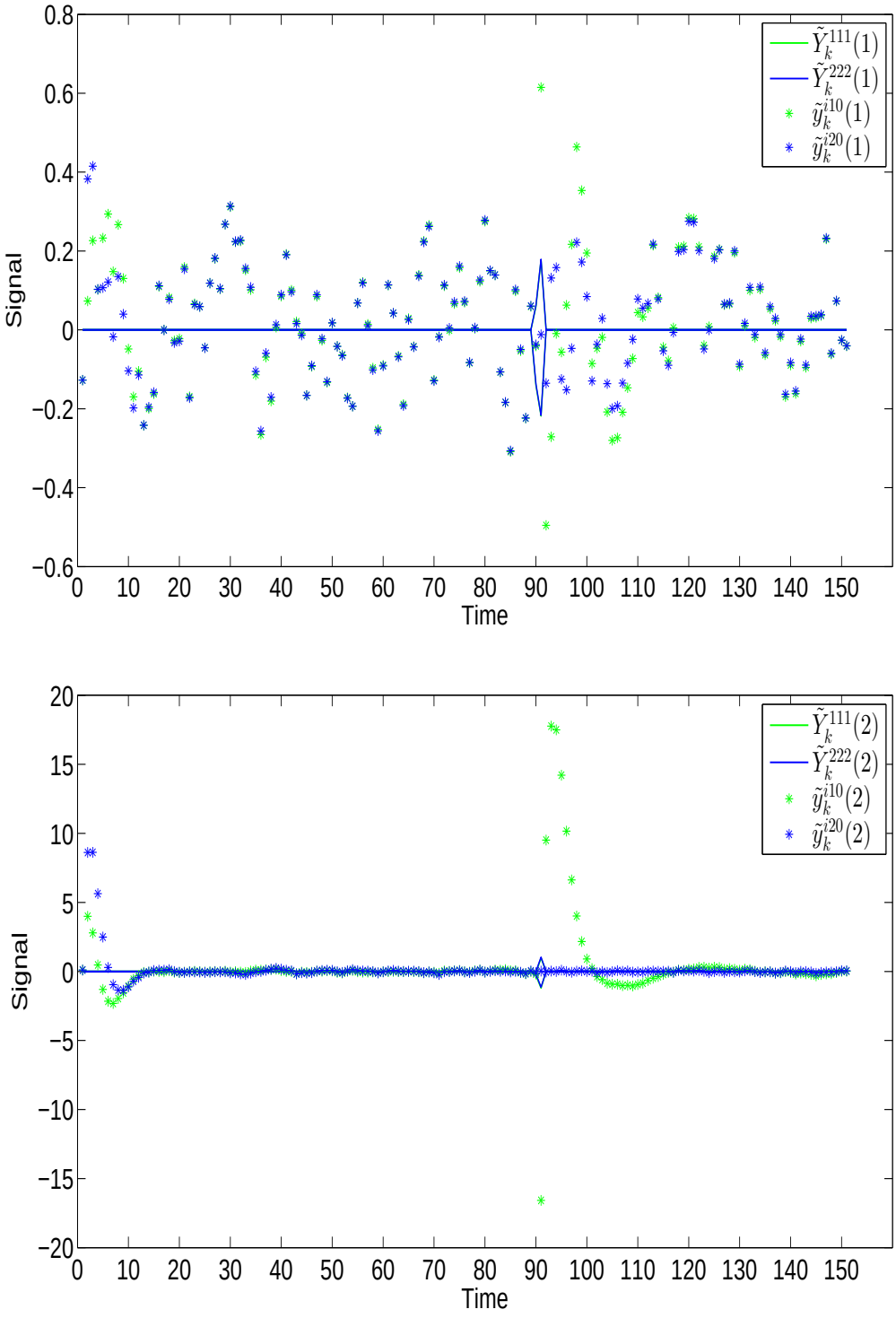


Figure 6.9: FI of Fault 2

- From time instants 0 to 75, the system is healthy and from time instants 76 to 150, the second actuator fault occurs.

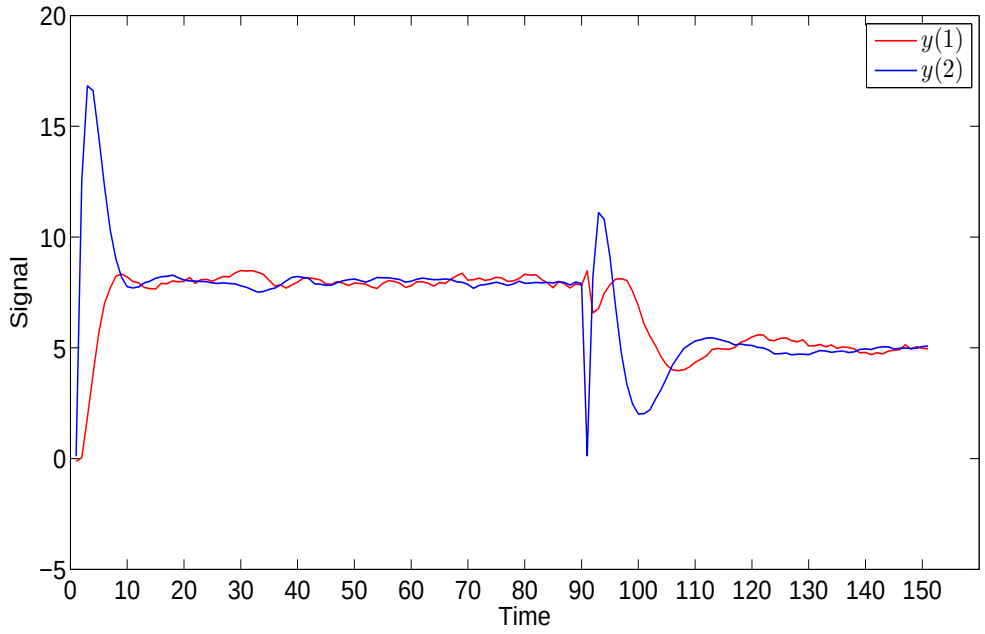


Figure 6.10: Outputs of Scenario 2

For these two scenarios, one needs to design the FI input and state and terminal constraint sets for the nominal MPC optimization problem of the healthy tube-based MPC controller, which are given as

$$\bar{U}_f^0 = \{u : \begin{bmatrix} 4.8 \\ 4.8 \end{bmatrix} \leq u \leq \begin{bmatrix} 5.2 \\ 5.2 \end{bmatrix}\},$$
$$\bar{X}_f^0 = \{x : \begin{bmatrix} -8.4767 \\ -0.9232 \end{bmatrix} \leq x \leq \begin{bmatrix} 8.4767 \\ 0.4232 \end{bmatrix}\},$$
$$\bar{X}_{fT}^{\ 0} = \{x : \begin{bmatrix} -8.4767 \\ -0.9232 \end{bmatrix} \leq x \leq \begin{bmatrix} 8.4767 \\ 0.4232 \end{bmatrix}\}.$$

Moreover, based on $\bar{U}_f^0$, the after-fault sets of output estimation errors of the two actuator-fault modes switched from the healthy mode can be constructed. Note that this example only takes the process from healthy to faulty as an example and does not consider system recovery. Thus, according to guaranteed FI conditions in Proposition 6.2, one only needs $\tilde{Y}^{110} \cap \tilde{Y}^{210} = \varnothing$, $\tilde{Y}^{120} \cap \tilde{Y}^{220} = \varnothing$, which are shown in Figure 6.3. This

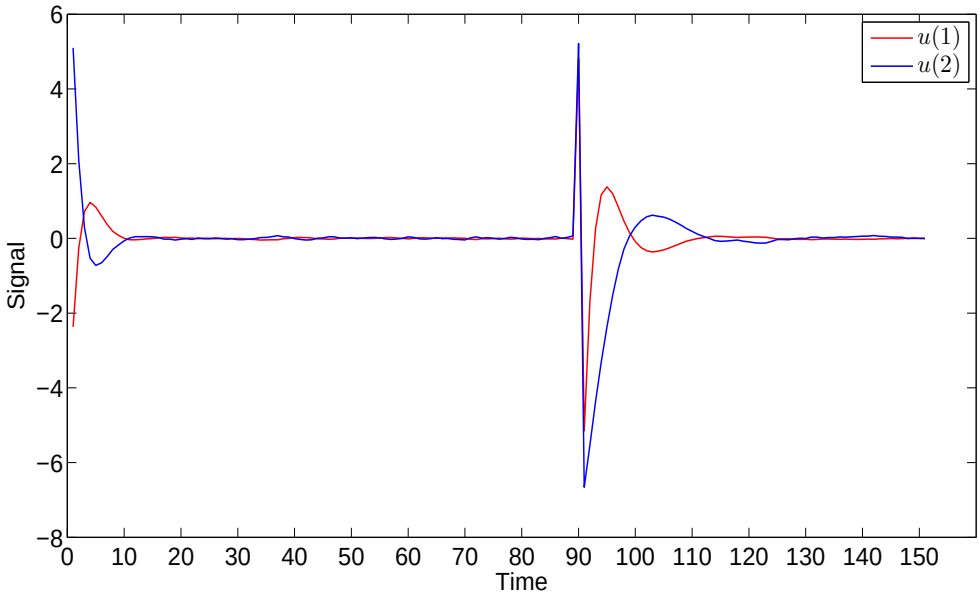


Figure 6.11: Inputs of Scenario 2

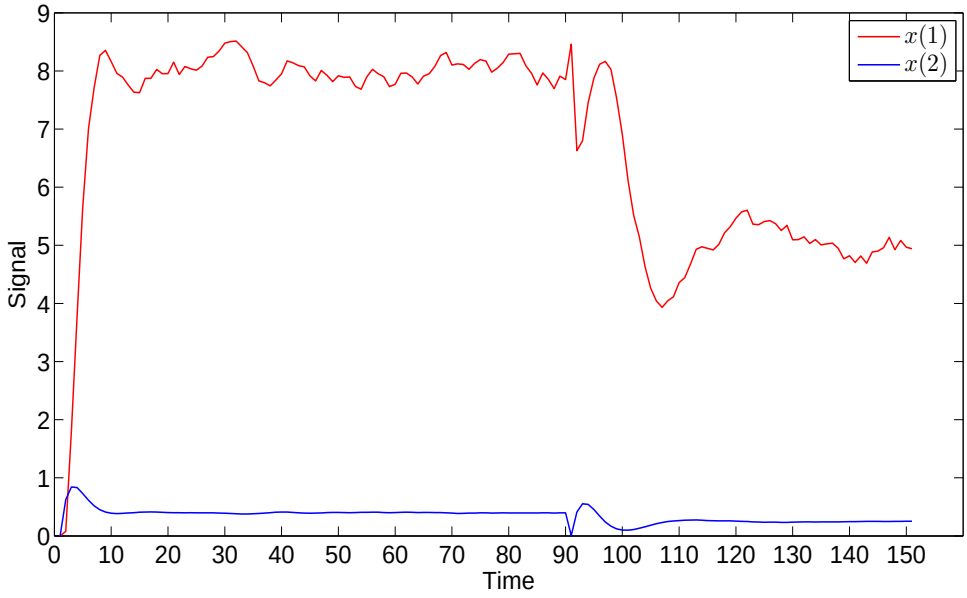


Figure 6.12: States of Scenario 2

implies that, after detection of either of both faults, it is guaranteed that the fault can be isolated by using the proposed active FI approach.

Remark 6.14. *For the proposed FDI approach, the FD and FI tasks are separate, which are based on different strategies. If the FD approach is not able to detect some considered actuator faults, it is not possible to tolerate the effect of these faults with the proposed AFTC strategy. Instead, only the PFTC ability of the controller can be used to tolerate these undetectable faults to some extent. In this example, this case will be illustrated by an undetectable fault.*

For the first fault scenario, the simulation results are shown in Figure 6.4. In Figure 6.4, $\tilde{y}_k^{i00}$ denotes the residual of the healthy observer (the first and third superscript indices of $\tilde{y}_k^{i00}$ are not important). The two plots in Figure 6.4 correspond to two different residual components, respectively. It is shown that the first actuator fault cannot be detected by the proposed FD approach. Thus, the active FI process is not started. The fault tolerance of this fault has to rely on the PFTC ability of the FTMPC scheme. Accordingly, the output tracking results of Scenario 1 are presented in Figure 6.5, which shows that, despite the first actuator fault cannot be detected, it can still be passively tolerated by the nominal MPC controller with satisfactory performance. Additionally, the states and outputs corresponding to this scenario are shown in Figures 6.6 and 6.6, respectively.

For the second scenario, the simulation results are shown in Figures 6.8, 6.9 and 6.10. In Figure 6.8, it is shown that the second actuator fault is detected at time instant 90. At the same time instant, the active FI process is started as seen in Figure 6.9. In Figure 6.9, $\tilde{y}_k^{i10}$ and $\tilde{y}_k^{i20}$ denote the residuals corresponding to the first and second observers, respectively. It is shown that, at time instant 91, $\tilde{y}_{91}^{i10} \notin \tilde{Y}_{91}^{110}$ and $\tilde{y}_{91}^{i20} \in \tilde{Y}_{91}^{220}$ hold, which implies that the second actuator is faulty. Once the second fault is isolated, the closed-loop system is reconfigured by using the corresponding MPC controller and the new state-input setpoint pair, which can be observed in Figure 6.10 that shows good tracking performance of the AFTC strategy under the second actuator fault. Additionally, the states and inputs are presented in Figures 6.12 and 6.11, which shows that the constraints are satisfied. Because of display space, please zoom in the second plot of Figure 6.9 to see clearly, despite the first plot of Figure 6.9 can already show the FI results.

Remark 6.15. *After system reconfiguration, the residual matching the new mode needs some time to enter and remain inside its corresponding set. In this case, if one restarts the FD mechanism at once. According to the proposed FD strategy, the system may give false fault alarms. In order to avoid this situation, whenever the system is reconfigured, a waiting time should be set (the waiting time describes the initial operating stage after reconfiguration. Thus, it can be defined based on the settling time of the system). During the waiting time, the FD mechanism is frozen till the waiting time elapses. Then, the FD mechanism is restarted again to monitor the new mode. In this example, a waiting time of* 20 *steps is set after system reconfiguration.*

6.6 Summary

In this chapter, an actuator FTMPC scheme is proposed, where tube-based MPC and the set-theoretic FDI are used. In the scheme, FD is passive based on invariant sets and FI is active by using MPC controllers and tubes. The proposed FTMPC scheme has relatively less computational complexity and less conservative FI conditions with respect to the passive approaches. Besides, for faults that the FD strategy cannot detect, the passive FTC ability of the scheme can still tolerate them to some extent in spite of a degree of possible performance degradation. However, for the proposed scheme, a key point is to design the input and state constraint sets for FI, which should be an important research point in the future.

Chapter 7

Fault-tolerant Model Predictive Control for Sensor Faults

In this chapter, a sensor FTMPC scheme based on min-max MPC and interval observers is proposed. In this scheme, min-max MPC can deal with system constraints and help to implement sensor FI, while interval observers can implement FDI and obtain robust state estimation for control action generation. This chapter ends up with an illustrative example, which can show the effectiveness of the proposed scheme.

7.1 Introduction

In Chapter 6, an actuator FTMPC scheme based on tube-based MPC is proposed, where the advantage of tube-based MPC consists in its relatively low complexity. When the system is in the steady-state operation of the i-th mode, tube-based MPC can indirectly guarantee input constraint satisfaction (i.e., $u_k \in U$) by directly confining the nominal input inside their sets (i.e., $\bar{u}_k^i \in \bar{U}^i$). But, if the system is at transient state induced by faults, the input constraint satisfaction may be violated even through the input constraint of the nominal system can be guaranteed. Comparatively, min-max MPC can directly manipulate the plant inputs and always confine the inputs inside a given set as long as MPC feasibility can be guaranteed. This is key for the proposed active sensor FI approach in the present scheme, which obtains FI by manipulating the plant inputs inside a designed input set.

Due to differences of characteristics of actuator and sensor faults, a direct extension of the proposed scheme in Chapter 6 to sensor faults is stiff. In this chapter, the objective is to propose a sensor FTMPC scheme that can make full use of sensor-fault characteristics for fault diagnosis. In this proposed sensor FTMPC scheme, FD is passive by interval observers, while FI is active based on the min-max MPC technique. In this way, the proposed scheme can simultaneously obtain input constraint satisfaction

and robust state estimation for control action generation. Most importantly, by using min-max MPC to directly manipulate the plant inputs, the effect of sensor faults on the outputs can be decoupled on-line in terms of FI (i.e., one sensor fault only corresponds to one output component). Thus, sensor FI can be reduced to search the output components affected by sensor faults. In [70], a multi-sensor FTMPC scheme is proposed, which tolerates the effect of sensor faults by switching among different groups of sensors. In some sense, this configuration has high economic price because of using more sensors and in this scheme FI implementation is passive, which generally increases fault diagnosis conservatism. The sensor FTMPC scheme proposed in this chapter is shown in Figure 7.1.

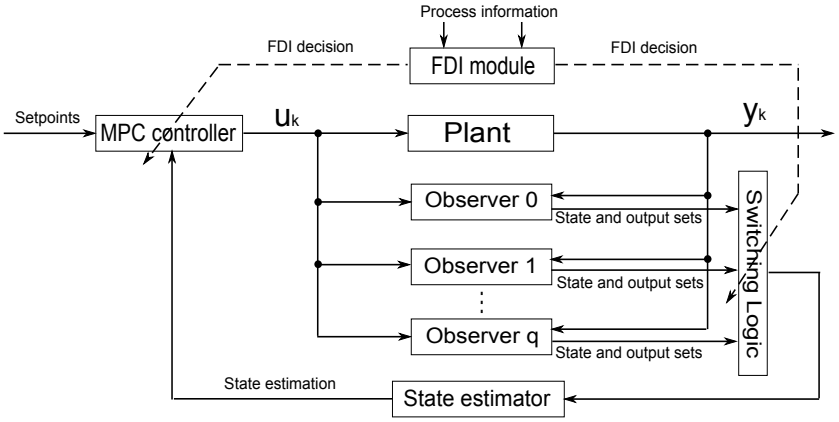


Figure 7.1: Sensor FTMPC scheme

This present FTMPC scheme has the following advantages. First, due to min-max robust MPC, the input bound of the plant can directly be manipulated to satisfy input constraint satisfaction to guarantee active FI during the transition induced by faults. Second, a robust state estimation approach for the MPC controller with feasibility guarantees is proposed. Third, this scheme can detect, isolate and tolerate unknown but bounded sensor faults with no need of physical multisensor redundancy.

7.2 Problem Formulation

7.2.1 Plant Models

In this chapter, the linear discrete time-invariant plant under the effect of sensor faults with unknown but bounded magnitudes is modelled as

$$x_{k+1} = Ax_k + Bu_k + \omega_k, \tag{7.1a}$$

$$y_k = \mathbf{G}_i C x_k + \eta_k. \tag{7.1b}$$

Remark 7.1. *In principle, with the method proposed in this chapter, one should be able to extend the sensor FDI approach proposed in Chapter 5 to the case of sensor faults with unknown but bounded magnitudes.*

Assumption 7.1. *The considered sensor faults can persist sufficiently long time such that the FDI module has enough responsive time to detect and isolate them.*

Remark 7.2. *As aforementioned, theoretically, the proposed scheme can deal with multiple faults. But, for brevity, one only considers single faults. Thus, one totally considers $q+1$ sensor modes including q sensor faults.*

In (7.1), the matrix $\mathbf{G}_i$ ($i \in \mathbb{I} = \{0, 1, ..., q\}$) models the i-th sensor mode (healthy or faulty), where $\mathbf{G}_0$ is the identity matrix denoting the healthy mode and $\mathbf{G}_i$ ($i \neq 0$) is a diagonal interval matrix modelling the i-th sensor fault with the form

$$\mathbf{G}_i = \begin{bmatrix} 1 & & & \\ & \ddots & \overset{i}{\downarrow} & \\ & & f_i & \\ & & & \ddots \\ & & & & 1 \end{bmatrix},$$

where the fault-modelling interval f_i satisfies $f_i \subseteq [0,\ 1)$. Moreover, an interval matrix describing all the considered sensor faults together is defined as

$$\mathbf{G}_f = \begin{bmatrix} f_1 & & & \\ & \ddots & & \\ & & f_i & \\ & & & \ddots \\ & & & & f_q \end{bmatrix},$$

where each diagonal element of $\mathbf{G}_f$ corresponds to the considered magnitude interval of one sensor fault. The system state and input constraints are considered, which are given as (6.2). The uncertainties ω_k and η_k in (7.1) are bounded as in (3.2) and (3.3), respectively.

Assumption 7.2. *The matrix A is a Schur and $(A, \mathbf{G}_i C)$ are detectable for all $i \in \mathbb{I}$.*

7.2.2 Setpoint Tracking

In the i-th sensor mode, the control objective of the closed-loop system is to track an output setpoint in the absence of uncertainties and/or faults, i.e.,

$$\lim_{k\to\infty} (y_k - y_i^*) \to 0,$$

where y_i^* denotes the given output setpoint corresponding to the i-th sensor mode.

Remark 7.3. *Sensor faults imply the loss of some available system information. Due to changes induced by sensor faults in the system, there may exist situations, where one has to degrade the expected performance, i.e., the given output setpoints may be different for different modes.*

In the proposed scheme, the state and input references for the i-th sensor mode are generated by the i-th reference model

$$x_{k+1}^{ref} = Ax_k^{ref} + Bu_k^{ref}, \tag{7.2a}$$
$$y_k^{ref} = \text{mid}(\mathbf{G}_i)Cx_k^{ref}, \tag{7.2b}$$

where mid$(\cdot)$ computes the middle-point matrix of an interval matrix, and u_k^{ref}, x_k^{ref} and y_k^{ref} are the reference input, state and output vectors at time instant k. By making use of (7.2), at steady state, one has

$$\begin{bmatrix} A-I & B \\ \text{mid}(\mathbf{G}_i)C & O \end{bmatrix} \begin{bmatrix} x_i^* \\ u_i^* \end{bmatrix} = \begin{bmatrix} O \\ y_i^* \end{bmatrix}. \tag{7.3}$$

Assumption 7.3. *Under the constraints (6.2), (7.3) is solvable for all $i \in \mathbb{I}$.*

In the i-th sensor mode, the solution (x_i^*, u_i^*) of (7.3) is the state-input setpoint pair corresponding to y_i^*. Thus, totally, $q+1$ pairs of state-input setpoints for $q+1$ sensor modes can be obtained. Note that, for each mode, (7.3) may have multiple solutions.

Remark 7.4. *If necessary, one can add the vectors ω^c and η^c into (7.2).*

7.3 Fault Detection and Isolation

7.3.1 Fault Detection

A bank of interval observers are designed to monitor the plant, each of which matches one considered sensor mode. The j-th ($j \in \mathbb{I}$) interval observer matching the j-th mode is designed as

$$\hat{X}_{k+1}^j = (A - L_j\mathbf{G}_jC)\hat{X}_k^j \oplus \{Bu_k\} \oplus \{L_jy_k\} \oplus (-L_j)V \oplus W, \tag{7.4a}$$
$$\hat{Y}_k^j = \mathbf{G}_jC\hat{X}_k^j \oplus V, \tag{7.4b}$$

where $\hat{X}_k^j$ and $\hat{Y}_k^j$ are the estimated state and output sets, and L_j is the observer gain that assures $A - L_j\mathbf{G}_jC$ is a Schur matrix (always possible under Assumption 7.2).

Assumption 7.4. *The initial state x_0 is inside an initial set $\hat{X}_0$ for all interval observers.*

As defined in (3.2), W and V are zonotopes. By defining $\hat{X}_0$ as a zonotope, $\hat{X}_{k+1}^j$ and $\hat{Y}_k^j$ are zonotopes as well. Using zonotope operations, the computational complexity of interval observers can be managed along the state dynamics evolution. Using zonotope properties, interval observers (7.4) can be propagated on-line by preserving zonotopic structure and guaranteeing containment. If the j-th interval observer matches the current mode, in the steady-state operation of this mode, one should have

$$x_k \in \hat{X}_k^j,$$
$$y_k \in \hat{Y}_k^j.$$

In the i-th mode, the i-th interval observer is selected by the system. To detect faults, the residual (in terms of sets) corresponding to the i-th mode is defined as

$$R_k^{ii} = y_k - \hat{Y}_k^i. \tag{7.6}$$

Remark 7.5. *Although a bank of interval observers operate concomitantly, only residual zonotopes of the interval observer matching the current mode is used for FD.*

As stated in Remark 7.5, when the system is in the i-th sensor mode, the FD task is implemented by testing whether or not

$$\mathbf{0} \in R_k^{ii} \tag{7.7}$$

is violated in real time. If a violation is detected, it means that a sensor fault has occurred. Otherwise, it is considered that the system is still in the i-th mode.

Note that the satisfaction of (7.7) does not always imply that the system is healthy because the FD strategy cannot be able to be sensitive to all of sensor faults. For undetectable faults, only the potential PFTC ability of the proposed scheme can be used to tolerate them to some extent.

7.3.2 Fault Isolation

7.3.2.1 Fault Isolation Conditions

If the system is open-loop, at time instant when a sensor fault occurs, the fault only affects the output component corresponding to the faulty sensor (i.e., one output component corresponds to one sensor). But, in the closed-loop system, due to the controller, the effect of sensor faults on the output components are masked and coupled, which increases difficulty for sensor fault diagnosis.

Different from the passive methods, the proposed FI approach in this chapter is active by impacting the effect of the controller on the plant to decouple the effect of different sensor faults on different output components on-line in terms of FI such that

one sensor fault only corresponds to one output component. To explain the proposed FI approach, it is assumed that the inputs of the plant are bounded by a zonotopic set

$$U_f = \{u \in \mathbb{R}^p : \left|u - u_f^c\right| \leq \bar{u}_f, u_f^c \in \mathbb{R}^p, \bar{u}_f \in \mathbb{R}^p\},$$

where U_f satisfies the hard input constraint of the plant

$$U_f \subseteq U. \tag{7.8}$$

Additionally, the output equation (7.1a) can be further rewritten as

$$x_{k+1} = Ax_k + \begin{bmatrix} B & I \end{bmatrix} \begin{bmatrix} u_k \\ \omega_k \end{bmatrix}. \tag{7.9}$$

Thus, by considering $u_k \in U_f$ and $\omega_k \in W$, an RPI set of the dynamics (7.9) can be constructed, which is denoted as X_f centered at

$$x_f^c = (I - A)^{-1}(Bu_f^c + \omega^c). \tag{7.10}$$

Furthermore, according to (7.1b), in the i-th sensor fault mode, the corresponding output set can be obtained as

$$Y_f^i = \mathbf{G}_i C X_f \oplus V,$$

where Y_f^i is centered at $y_f^{c,i} = \text{mid}(\mathbf{G_i})Cx_f^c + \eta^c$. If $\mathbf{G}_i$ in (7.1a) takes the value $\mathbf{G}_0$, the corresponding output set in the healthy mode is

$$Y_f^0 = CX_f \oplus V,$$

where Y_f^0 is centered at $y_f^{c,0} = Cx_f^c + \eta^c$. The output set has q components, each of which is an interval that can be obtained by projecting the output set towards the corresponding dimension.

In terms of $u_k \in U_f$, only the i-th component of Y_f^i is different from that of Y_f^0 because of the effect of the i-th sensor fault, while all the other components are the same. Furthermore, in contrast to Y_f^0, one defines a set

$$Y_f = \mathbf{G}_f C X_f \oplus V,$$

where Y_f describes all the considered sensor faults and is centered at $y_f^c = \text{mid}(\mathbf{G}_f)Cx_f^c + \eta^c$. By comparing Y_f^0, Y_f^i with Y_f, it can be observed that:

- All the interval components of Y_f^0 are different from those of Y_f, respectively.
- Only the i-th interval component of Y_f^i ($i \neq 0$) is the same as that of Y_f, while all the other components are different from those of Y_f.

For brevity, the l-th interval components of Y_f^0, Y_f^i and Y_f are denoted as $Y_f^0(l)$, $Y_f^i(l)$ and $Y_f(l)$, which are centered at $y_f^{c,0}(l)$, $y_f^{c,i}(l)$ and $y_f^c(l)$ (denote the l-th components of $y_f^{c,0}$, $y_f^{c,i}$ and y_f^c), respectively.

Proposition 7.1. *For the plant (7.1) under the constraints (6.2), if there exists a set U_f that satisfies (7.8) such that*

$$Y_f^0(l) \cap Y_f(l) = \varnothing$$

for all $l \in \mathbb{I} \setminus \{0\}$, all the considered sensor modes can be isolated after their detection.

Proof : If the inputs are bounded by U_f, because of the separation of the l-th interval components, i.e, $Y_f^0(l) \cap Y_f(l) = \varnothing$, once the l-th fault has occurred, the l-th output component finally enters into the l-th interval of $Y_f(l)$ instead of $Y_f^0(l)$, while all the other output components enter into the corresponding components of $Y_f^0(l)$ instead of $Y_f(l)$, respectively, which indicates the l-th fault. □

Assumption 7.5. *There exists an input set $U_f \subseteq U$ such that all the considered sensor modes can satisfy Proposition 7.1.*

7.3.2.2 Fault Isolation Strategy

It is known that sensor faults do not change the dynamics of the plant. Thus, if a sensor fault is detected at time instant k_d, the current state of the plant is still inside X_M (X_M is defined as the MRCI set of the dynamics (7.1a) under constraints (6.2)), i.e.,

$$x_{k_d} \in X_M. \tag{7.11}$$

At time instant k_d, the proposed FI approach switches the input constraint of the min-max MPC controller from U to U_f to start active FI. After constraint switching, if the MPC controller is feasible, the generated control action should satisfy

$$u_{k_d} \in U_f. \tag{7.12}$$

In order to isolate a fault during the transition induced by the fault, at the FD time k_d, one initializes a set-based dynamics

$$X_{k+1} = AX_k \oplus Bu_k \oplus W, \tag{7.13a}$$
$$Y_k = \mathbf{G}_f C X_k \oplus V \tag{7.13b}$$

with $X_{k_d} = X_M$ at time instant k_d and $u_k \in U_f$ ($k \geq k_d$). Afterwards, the state and output set sequences can be generated by (7.13). Moreover, by using $\check{X}_{k_d} = X_M$ at time instant k_d to initialize the other set-based dynamics

$$\check{X}_{k+1} = A\check{X}_k \oplus BU_f \oplus W, \tag{7.14a}$$
$$\check{Y}_k = \mathbf{G}_f C \check{X}_k \oplus V, \tag{7.14b}$$

the other state and output set sequences can be generated by (7.14). The state set sequence generated by (7.14a) will converge to the mRPI set of the dynamics (7.1a) with respect to $u_k \in U_f$ and $\omega_k \in W$, enter into and stay inside X_f. Correspondingly, the output set sequence generated by (7.14b) will finally enter into and stay inside Y_f.

Proposition 7.2. *At the FD time instant k_d, by using X_M to initialize (7.13) and (7.14) and comparing (7.13) with (7.14), for all $k \geq k_d$, $X_k \subseteq \check{X}_k$ and $Y_k \subseteq \check{Y}_k$ always hold.*

Proof : Comparing (7.13) with (7.14), it can be observed that (7.14) is a set-based dynamics of (7.13) by considering the input set U_f during active FI process. Moreover, with X_M to initialize both (7.13) and (7.14) at time instant k_d, i.e., $X_{k_d} \subseteq \check{X}_{k_d}$, it can be obtained, for all $k \geq k_d$, $X_k \subseteq \check{X}_k$ and $Y_k \subseteq \check{Y}_k$ will always hold. □

Under Proposition 7.2, considering (7.11) and (7.12), one has the conclusion presented in Proposition 7.3.

Proposition 7.3. *Given the plant (7.1), the state and output set sequences generated by (7.13), starting from the FD time k_d, $x_k \in X_k$ can hold for all $k \geq k_d$. If the plant is healthy, no components of y_k and Y_k can persistently satisfy $y_k(l) \in Y_k(l)$ ($l \in \mathbb{I} \setminus \{0\}$) for all $k \geq k_d$, while if the l-th fault has occurred, the l-th components of y_k and Y_k can satisfy $y_k(l) \in Y_k(l)$ for all $k \geq k_d$ but all the other components of y_k and Y_k cannot.*

Proof : First, because of (7.11), (7.12) and $u_k \in U_f$ for all $k \geq k_d$, comparing (7.1) with (7.13), $x_k \in X_k$ will hold for all $k \geq k_d$. Second, under Proposition 7.2, comparing (7.14) with (7.13), X_k and Y_k finally enter into X_f and Y_f and stay inside, respectively. For the l-th sensor-fault mode, under the FI conditions in Proposition 7.1, starting from the FD time k_d, only $y_k(l) \in Y_k(l)$ will hold for all $k \geq k_d$ with the initialization $X_{k_d} = X_M$, while all the other components of y_k do not have the same conclusion. For the healthy mode, since all the components of Y_f^0 are separate from the corresponding components of Y_f, respectively, no components of y_k can be contained by the corresponding interval of Y_k for all $k \geq k_d$. □

Thus, under FI conditions proposed in Propositions 7.1, 7.3 and Assumption 7.5, if a considered sensor fault is detected, by using the output sets generated by (7.13), the fault can be isolated by real-time testing whether or not

$$y_k(l) \in Y_k(l),\ k \geq k_d \tag{7.15}$$

is violated for all $l \in \mathbb{I} \setminus \{0\}$. According to the real-time testing of (7.15) for all the components, one can have the FI conclusions:

- If the plant recovers to the health from a faulty mode, for $k \geq k_d$, by testing (7.15), at a time instant when all the output components violate (7.15), it implies that the healthy mode is isolated at this time instant.

- If the plant changes into another fault from a faulty mode or the healthy mode, only the output component corresponding to the occurring faulty mode can always respect (7.15) while all the others will finally diverge from the corresponding interval components of Y_k, respectively. Thus, the proposed FI approach consists in searching this component that indicates the fault and the corresponding time instant that indicates the FI time.

7.4 Fault-tolerant Control

7.4.1 Model Predictive Controller

In this proposed scheme, the robust MPC controller is implemented by using the min-max MPC technique, which is introduced in Chapter 2. In the steady-state operation of the i-th mode, the i-th state-input setpoint pair and the i-th interval observer are used in the closed-loop system and the corresponding robust MPC controller is designed as

$$\begin{aligned} J_k = \min_{\mathbf{u}} \max_{\mathbf{w}} & \sum_{j=0}^{N-1} \|(x_{k+j|k} - x_i^*)\|_Q^2 + \|(u_{k+j|k} - u_i^*)\|_R^2 + \|(x_{k+N|k} - x_i^*)\|_P^2 \\ \text{subject to} \quad & \left.\begin{aligned} x_{k+j|k} &\in X, \\ u_{k+j|k} &\in U, \\ x_{k+N|k} &\in X_M, \\ x_{k|k} &= \hat{x}_k, \end{aligned}\right\} \forall \omega_{k+j|k} \in W, \end{aligned} \tag{7.16}$$

where N is the prediction horizon, $\mathbf{u} = [u_{k|k}, u_{k+1|k}, \ldots, u_{k+N-1|k}]$, $\mathbf{w} = [\omega_{k|k}, \omega_{k+1|k}, \ldots, \omega_{k+N-1|k}]$, Q, R and P are positive-definite weighting matrices and the internal model of the MPC controller is given as

$$x_{k+j+1|k} = Ax_{k+j|k} + Bu_{k+j|k} + \omega_{k+j|k}.$$

In the i-th mode, if no fault is detected, the MPC controller is used to robustly control the system to track the i-th output setpoint y_i^* (see (7.16)). If a fault is detected, at the FD time, active FI is started by switching the input and terminal state constraints of (7.16) from U and X_M to U_f and X_{M_f}, respectively, i.e.,

$$\begin{aligned} J_k = \min_{\mathbf{u}} \max_{\mathbf{w}} & \sum_{j=0}^{N-1} \|(x_{k+j|k} - x_i^*)\|_Q^2 + \|(u_{k+j|k} - u_i^*)\|_R^2 + \|(x_{k+N|k} - x_i^*)\|_P^2 \\ \text{subject to} \quad & \left.\begin{aligned} x_{k+j|k} &\in X, \\ u_{k+j|k} &\in U_f, \\ x_{k+N|k} &\in X_{M_f}, \\ x_{k|k} &= \hat{x}_k, \end{aligned}\right\} \forall \omega_{k+j|k} \in W. \end{aligned} \tag{7.17}$$

By means of active FI, once a sensor fault can be isolated, the system is correspondingly reconfigured by the MPC controller indicated in (7.16) with the state-input setpoint pair and interval observer corresponding to the new sensor mode.

Remark 7.6. *As mentioned in Chapter 2, the main advantage of min-max MPC with respect to tube-based MPC consists in that it can directly deal with the plant constraint. As long as a min-max MPC controller is feasible, the plant constraints can always be guaranteed during both steady and transient state as seen in (7.16) and (7.17). This feature is the key to decouple the effect of different sensor faults on different output components in terms of sensor FI.*

7.4.2 Robust State Estimation

Under the constraints (6.2), one can construct the MRCI set X_M for the plant (7.1). Since X_M is used as the terminal state constraint of the MPC controller (7.16), ideally, if the initial state is inside X_M and the real states are available for the MPC controller updating, the states can always be confined inside X_M and the MPC controller can always be feasible. Unfortunately, it is impossible to obtain the real states. Instead, one has to estimate the states and use state estimation for the updating of the MPC controller.

7.4.2.1 State Estimation

For feasibility and stability of the MPC controller with state estimation, one still uses the MRCI set X_M as the terminal state constraint at steady state in the proposed scheme as in (7.16).

Proposition 7.4. *In the steady-state operation, as long as the MPC controller (7.16) is updated by a point inside X_M at each time instant, i.e., $\hat{x}_k \in X_M$, it can keep feasible such that the generated control actions always satisfy $u_k \in U$.*

Proof : This can be understood according to the definition of the MRCI set. □

Furthermore, in order to guarantee that the states can always be inside the constraint set X, one makes the following assumptions.

Assumption 7.6. *The mRPI set (denoted as X_m) corresponding to $u_k \in U$ and $\omega_k \in W$ for the dynamics (7.9) is contained in the set X.*

Assumption 7.7. *There exists $\alpha \geq 1$ such that the initial state x_0 of (7.1a) satisfies $x_0 \in \bar{X} = \alpha X_m$ and $\bar{X} \subset X_M$.*

Remark 7.7. *At steady state, the MPC controller can guarantee constraint satisfaction. But, during the transition induced by faults, one cannot make the same conclusion, Thus, Assumptions 7.6 and 7.7 are especially made to guarantee constraint satisfaction at transient state.*

Thus, in the steady-state operation, because of $u_k \in U$, the states always stay inside $\bar{X}$. Furthermore, if the system is in the steady-state operation of the i-th mode, the i-th interval observer can real-time estimate sets to contain the current system states, i.e.,

$$x_k \in \hat{X}_k^i.$$

Thus, based on $\bar{X}$ and $\hat{X}_k^i$, one has

$$x_k \in \bar{X} \cap \hat{X}_k^i. \tag{7.18}$$

In the i-th steady-state mode, the following method is used to obtain the state estimation, i.e.,

$$\hat{x}_k = \text{center}(\bar{X} \cap \hat{X}_k^i), \tag{7.19}$$

where $\hat{x}_k$ is the estimation of x_k, which is used to update the MPC controller (7.16) to generate control actions at each time instant.

Remark 7.8. *Actually, any point inside the set $\bar{X} \cap \hat{X}_k^i$ can be used as the state estimation. But, for brevity, one selects the center as given in (7.19). If $\bar{X} \cap \hat{X}_k^i$ is not centered, center$(\bar{X} \cap \hat{X}_k^i)$ denotes the center of the convex hull of $\bar{X} \cap \hat{X}_k^i$.*

Proposition 7.5. *Under Assumption 7.6, the optimization problem (7.16) of the MPC controller with the state estimation (7.19) is recursively feasible in the steady-state operation. Moreover, the real states x_k are always confined inside $\bar{X}$.*

Proof : Under Assumption 7.6, $\bar{X}$ is contained inside X_M, which implies $\hat{x}_k \in X_M$ according to the definition of the RPI set. Thus, at each step, with (7.19), the MPC controller (7.16) is always feasible. If the MPC controller is feasible, $u_k \in U$ always holds, which always implies that the states will still stay inside their RPI set, i.e., $x_k \in \bar{X} \subseteq X$. □

7.4.2.2 Stability with State Estimation

When using the state estimation (7.19) to update the MPC controller, there always exist state estimation errors that are defined as

$$\tilde{x}_k = x_k - \hat{x}_k, \tag{7.20}$$

Since both x_k and $\hat{x}_k$ are confined in the intersection $\bar{X} \cap \hat{X}_k^i$, $\tilde{x}_k$ should be bounded. In the worst case, i.e., $\bar{X}$ coincides with $\hat{X}_k^i$, the bound of $\tilde{x}_k$ can be obtained as

$$\tilde{x}_k \in \bar{X} \oplus (-\bar{X}). \tag{7.21}$$

Note that, because the coincidence of $\bar{X}$ and $\hat{X}_k^i$ is a low probability event, the real-time bound of $\tilde{x}_k$ is less conservative than (7.21). Since the plant is assumed to be stable for RPI set construction as in Assumption 7.2, the bounding of $\tilde{x}_k$ also implies stability of the system with the state estimation (7.19).

7.4.3 Fault-tolerant Control Approach

7.4.3.1 Active Fault Isolation

As aforementioned, once a sensor fault (indexed by j ($j \neq i$)) is detected at time instant k_d, the proposed FI approach activates FI by switching the constraints of the MPC controller from U and X_M to U_f and X_{M_f}, respectively.

Proposition 7.6. *Under Assumptions 7.5 and 7.6, the mRPI set (denoted as X_{m_f}) for the dynamics (7.9) corresponding to $u_k \in U_f$ is contained in X_m. Moreover, X_{M_f} is an RCI set for the dynamics (7.9) corresponding to $u_k \in U$.*

Proof : Because of $U_f \subseteq U$, the mRPI set for the dynamics (7.9) corresponding to $u_k \in U_f$ should be contained in the mRPI set corresponding to $u_k \in U$. Furthermore, both mRPI sets are contained in X. For $U_f \subseteq U$, X_{M_f} can satisfy the definition as an RCI set of the system corresponding to $u_k \in U$, which indicates $X_{M_f} \subseteq X_M$. □

After input constraint set switching, it is not guaranteed that $x_k \in \hat{X}_k^i$ can always hold during active FI, which implies that (7.19) cannot guarantee the feasibility of the MPC controller (7.17). Thus, it is necessary to propose a new strategy to update the MPC controller to guarantee active FI and feasibility at transient state. In order to avoid infeasibility of (7.17) during active FI, for each step $k \geq k_d$, one uses

$$\hat{x}_k = \text{center}(X_{M_f}) \tag{7.22}$$

as state estimation to update (7.17) to generate control actions for FI implementation.

By means of (7.22), during active FI, the feasibility of the MPC controller can always be guaranteed, i.e., $u_k \in U_f$, which implies the satisfaction of the FI conditions given in Proposition 7.1 on-line. Furthermore, FI can be implemented by using the FI approach (7.15). One should realize when using the state estimation (7.22) to update the MPC controller (7.17) instead of using the real states, there always exist errors. In spite of the errors, there are several reasons that support this strategy.

- By using (7.22) to update the MPC controller, the generated control law u_k keeps constant, i.e., the injection of a step signal to the plant. Since the plant is stable, the errors will not be amplified and the system can always keep stable.
- During active FI, MPC feasibility implies $u_k \in U_f$. Thus, the states finally converge into X_f and stay inside, which has no relevance to the aforementioned errors.
- Since the proposed FI strategy can isolate faults and reconfigure the system during the transition induced by the faults, a short FI time can limit the effect of the errors.

At time instant k_i when the fault is isolated (assume it is the j-th mode), the MPC constraints of (7.17) are switched back to U and X_M from U_f and X_{M_f}, respectively (i.e., (7.16)).

Proposition 7.7. *At the FI time k_i, $x_{k_i} \in \bar{X}$ (i.e., $x_{k_i} \in X_M$). Furthermore, the MPC controller is always feasible and $x_k \in X_M$ for all $k \geq k_i$.*

Proof : Because of $x_k \in \bar{X} \subseteq X_M$ in the steady-state operation. At the FD time k_d, although the constraints U and X_M are switched into U_f and X_{M_f}, respectively, one still has $u_k \in U_f \subseteq U$ with (7.22), which implies that the states still stay inside $\bar{X}$. At the FI time k_i when the constraints are switched back into U and X_M, $x_{k_i} \in \bar{X}$ still holds and the feasibility of (7.16) assures $x_k \in X_M$ for all $k \geq k_i$. □

Remark 7.9. *It is assumed that the j-th mode ($j \neq i$) is isolated. Under Proposition 7.7, at time instant k_i, if the j-th interval observer satisfies $x_{k_i} \in \hat{X}_{k_i}^j$, the state estimations similar with (7.19) can be directly used for the new MPC controller and the FD mechanism based on the j-th interval observer is restarted for $k \geq k_i$. If $x_{k_i} \notin \hat{X}_{k_i}^j$, the strategy similar to (7.22) is firstly used to guarantee the feasibility of the new MPC controller for $k \geq k_i$ till a time instant when $x_k \in \hat{X}_k^j$ holds. Then, the state estimation (7.19) starts to be used for the new MPC controller and the FD mechanism based on the j-th interval observer is restarted.*

Remark 7.9 mentions the feasibility problem during the initial phase after system reconfiguration. However, since the real state x_{k_i} is unknown, one cannot use the strategy in Remark 7.9 to guarantee the feasibility and the accurate restarting of the FD mechanism. But, because one knows that $x_{k_i} \in X_M$ holds, one can re-initialize the j-th interval observer and then directly use (7.19) at the FI time instant to guarantee the recursive feasibility after reconfiguration.

Proposition 7.8. *When the j-th sensor mode is isolated at the FI time k_i, one can use X_M to re-initialize the dynamics of the j-th interval observer, i.e.,*

$$\hat{X}_{k_i}^j = X_M.$$

In this way, the state estimation(7.19) corresponding to the j-th interval observer can be directly used for the updating of the new MPC controller and the FD mechanism based on the j-th interval observer is restarted for $k \geq k_i$.

In additional to Proposition 7.8, one can use another different strategy to guarantee feasibility of the MPC controller and avoid false fault alarms during the initial stage after reconfiguration, which is summarized in Proposition 7.9.

Proposition 7.9. *It is assumed that the j-th mode ($j \neq i$) is isolated. Under Proposition 7.7, for $k \geq k_i$, if the intersection $\bar{X} \cap \hat{X}_k^j$ is not empty, $\hat{x}_k = center(\bar{X} \cap \hat{X}_k^j)$ is used for the MPC controller, otherwise, (7.22) continues to be used. It is guaranteed that, several steps later after reconfiguration, $\bar{X} \cap \hat{X}_k^j \neq \varnothing$ can persistently hold.*

7.4.4 Fault-tolerant Control Algorithm

As previously discussed, an FTC algorithm is summarized for the proposed FTMPC scheme, which is presented as follows:

- It is assumed that the system is in the i-th mode, i.e., the i-th state-input setpoint pair is used for tracking and the i-th interval observer is used for FD and robust state estimation.
- When a fault is detected at time instant k_d, the MPC controller is simultaneously switched to (7.17) from (7.16). Here, (7.22) is used to guarantee feasibility of (7.17) and active FI, (7.13) is initialized by X_M to generate the output set sequence for the FI strategy (7.15) to isolate the fault.

- Once the fault is isolated (it is assumed that the index is j ($j \neq i$)), the system is reconfigured and the strategy proposed in Propositions 7.8 or 7.9 is used for the new mode. Afterwards, the whole algorithm is repeated to monitor the new mode.

Remark 7.10. *In the same principle, this sensor FTC scheme can also deal with sensor recovery from faulty to healthy.*

Remark 7.11. *Interval observer implementation and set computation in this scheme are fully based on zonotopes. Please see Chapter 2 for zonotope properties and operations.*

7.5 Illustrative Example

In this section, one also takes the circuit in [41] as an example. The chart and system matrices of the circuit can be seen in (6.32) and Figure 6.2. However, different from the circuit in Chapter 6, one considers sensor faults instead of actuator faults here and uses a different group of parameters. The values of relevant parameters in (6.32) and Figure 6.2 are given as $R_1 = 30\Omega$, $R_2 = 1000\Omega$, $R_3 = 20\Omega$, $L = 80\text{mH}$, $C_p = 50\mu\text{F}$, $R_{eq} = R_1 + R_2$ and $\alpha_1 = \alpha_2 = 1$. With a sampling time of $1/15\text{s}$, the dynamics of the circuit can be discretized as

$$x_{k+1} = A_d x_k + B_d u_k + E_d w_k, \tag{7.23a}$$
$$y_k = \mathbf{G}_i C_d x_k + \eta_k, \tag{7.23b}$$

where

$$A_d = \begin{bmatrix} 0.8706 & 3.8835 \\ -0.0024 & 0.2395 \end{bmatrix}, B_d = \begin{bmatrix} 0.1294 & 0.0667 \\ -0.0809 & 0.0833 \end{bmatrix}, E_d = \begin{bmatrix} 0.1294 \\ 0.0024 \end{bmatrix}, C_d = \begin{bmatrix} 1 & 0 \\ 0 & 20 \end{bmatrix}.$$

Moreover, in (7.23), the process disturbances and measurement noises of the circuit are bounded, which are given as $|\omega| \leq 1.5$ and $|\eta| \leq \begin{bmatrix} 0.1 & 0.1 \end{bmatrix}^T$. Besides, in this example, all the relevant designing parameters are presented as follows:

- Observer gains[1]:

$$L_0 = \begin{bmatrix} 0.4706 & 0.1942 \\ -0.0024 & -0.013 \end{bmatrix}, L_1 = \begin{bmatrix} 9.4110 & 0.1942 \\ -0.0485 & -0.013 \end{bmatrix}, L_2 = \begin{bmatrix} 0.4706 & 3.8835 \\ -0.0024 & -0.2605 \end{bmatrix}.$$

- Considered fault magnitudes:

$$\mathbf{G}_1 = \begin{bmatrix} [0, 0.1] & 1 \\ 0 & 1 \end{bmatrix}, \mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 0 & [0, 0.1] \end{bmatrix}, \mathbf{G}_f = \begin{bmatrix} [0, 0.1] & 0 \\ 0 & [0, 0.1] \end{bmatrix}.$$

- Actual fault magnitudes[2]: $G_1 = \begin{bmatrix} 0.05 & 1 \\ 0 & 1 \end{bmatrix}, G_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0.05 \end{bmatrix}$.

[1] L_1 and L_2 are obtained using $\text{mid}(\mathbf{G}_1)$ and $\text{mid}(\mathbf{G}_2)$, respectively.

[2] G_1 and G_2 denote the actual fault magnitudes, i.e., $G_1 \in \mathbf{G}_1$ and $G_2 \in \mathbf{G}_2$. Note that the occurrence of any fault magnitude inside $\mathbf{G}_1$ and $\mathbf{G}_2$ can be isolated if they can be detected.

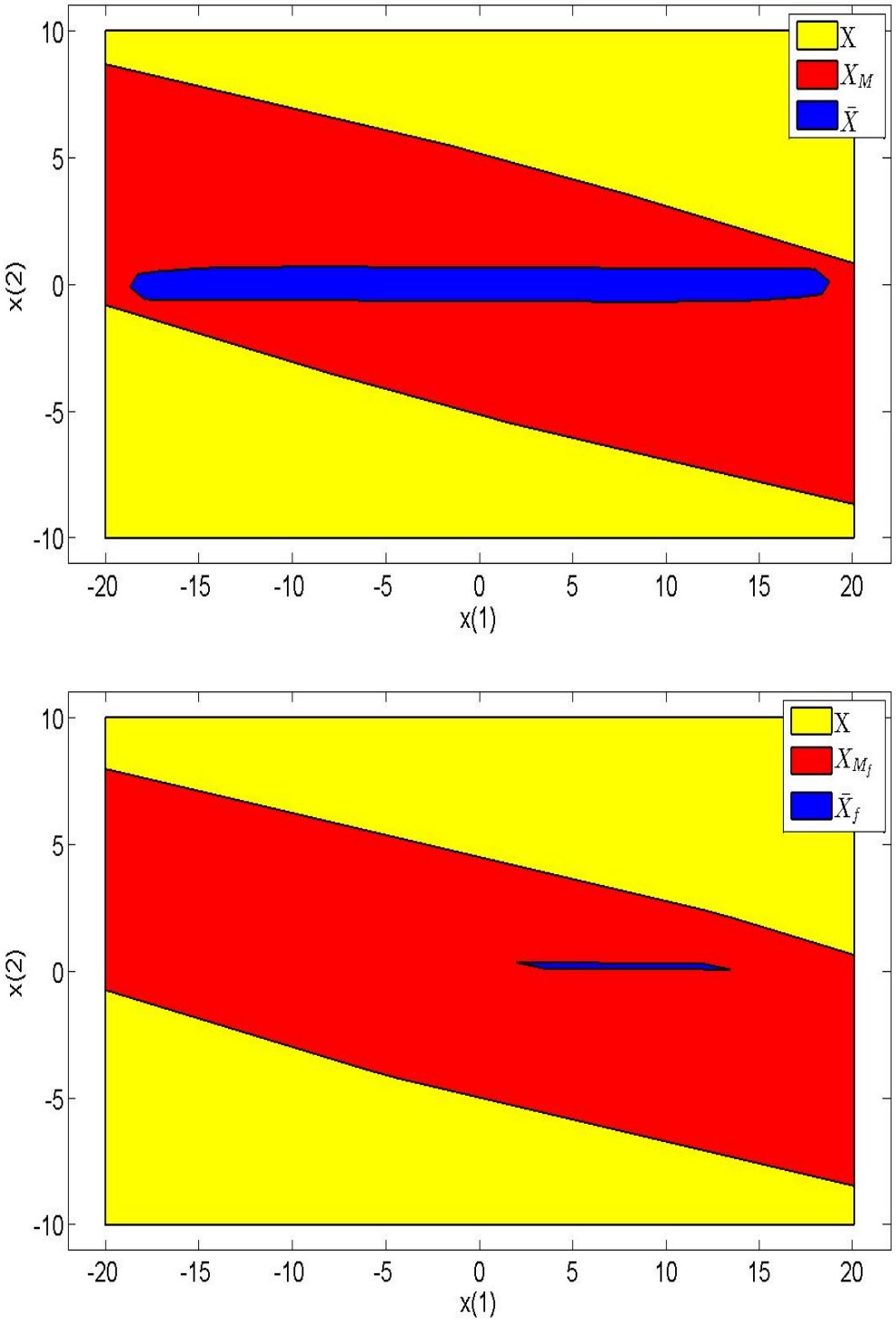


Figure 7.2: Relevant state sets

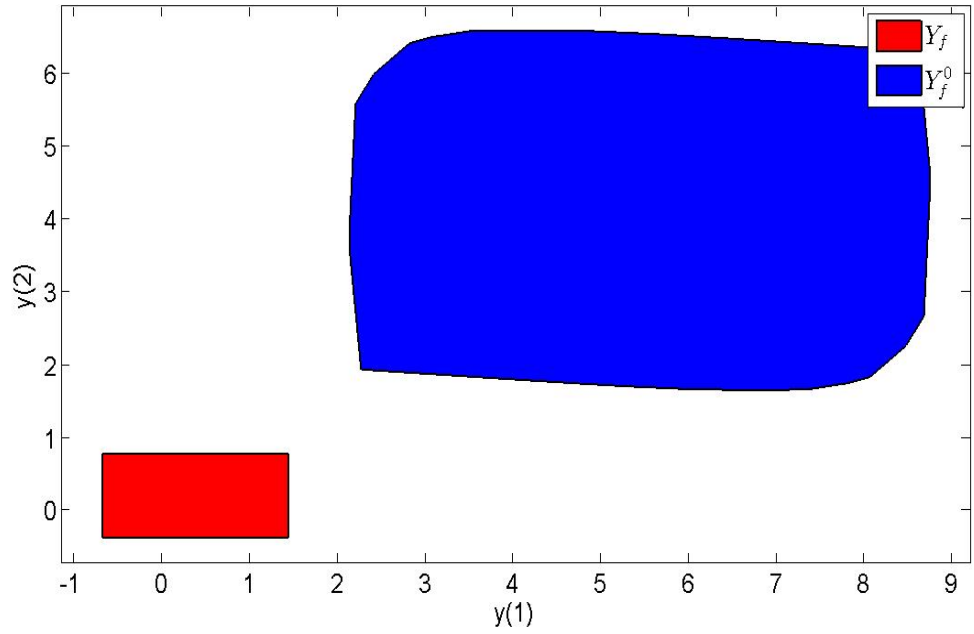


Figure 7.3: Output sets for active FI

- Output setpoints: $y_0^* = \begin{bmatrix} 4 \\ 2 \end{bmatrix}, y_1^* = \begin{bmatrix} 0 \\ 2 \end{bmatrix}, y_2^* = \begin{bmatrix} 4 \\ 0 \end{bmatrix}$.
- State-input setpoint pairs:

$$u_0^* = \begin{bmatrix} 0.313 \\ 1.333 \end{bmatrix}, u_1^* = \begin{bmatrix} -2.313 \\ -1.333 \end{bmatrix}, u_2^* = \begin{bmatrix} 2.627 \\ 2.667 \end{bmatrix}, x_0^* = \begin{bmatrix} 4 \\ 0.1 \end{bmatrix}, x_1^* = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix}, x_2^* = \begin{bmatrix} 4 \\ 0 \end{bmatrix}.$$

- Initial conditions: $x_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \hat{X}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix} \mathbb{B}^2$.
- System constraints: $U = \{u : \begin{bmatrix} -3 \\ -3 \end{bmatrix} \leq u \leq \begin{bmatrix} 3 \\ 3 \end{bmatrix}\}, X = \{x : \begin{bmatrix} -20 \\ -10 \end{bmatrix} \leq x \leq \begin{bmatrix} 20 \\ 10 \end{bmatrix}\}$.
- Input set for active FI: $U_f = \{u_k : \begin{bmatrix} 0 \\ 2 \end{bmatrix} \leq u \leq \begin{bmatrix} 1 \\ 3 \end{bmatrix}\}$.
- Prediction horizon: $N = 2$.
- MPC controller parameters: $Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix}, P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

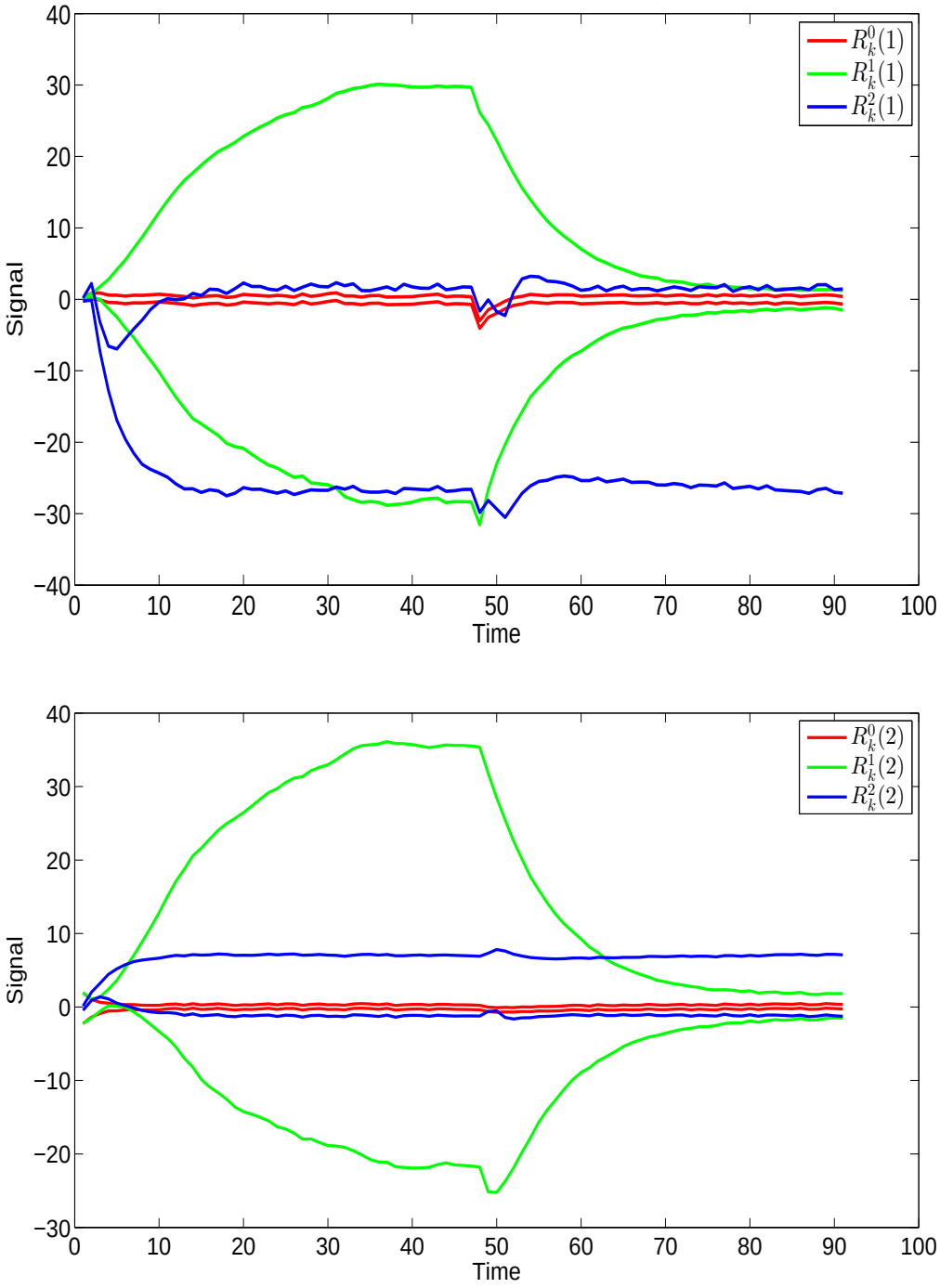


Figure 7.4: FD of Fault 1

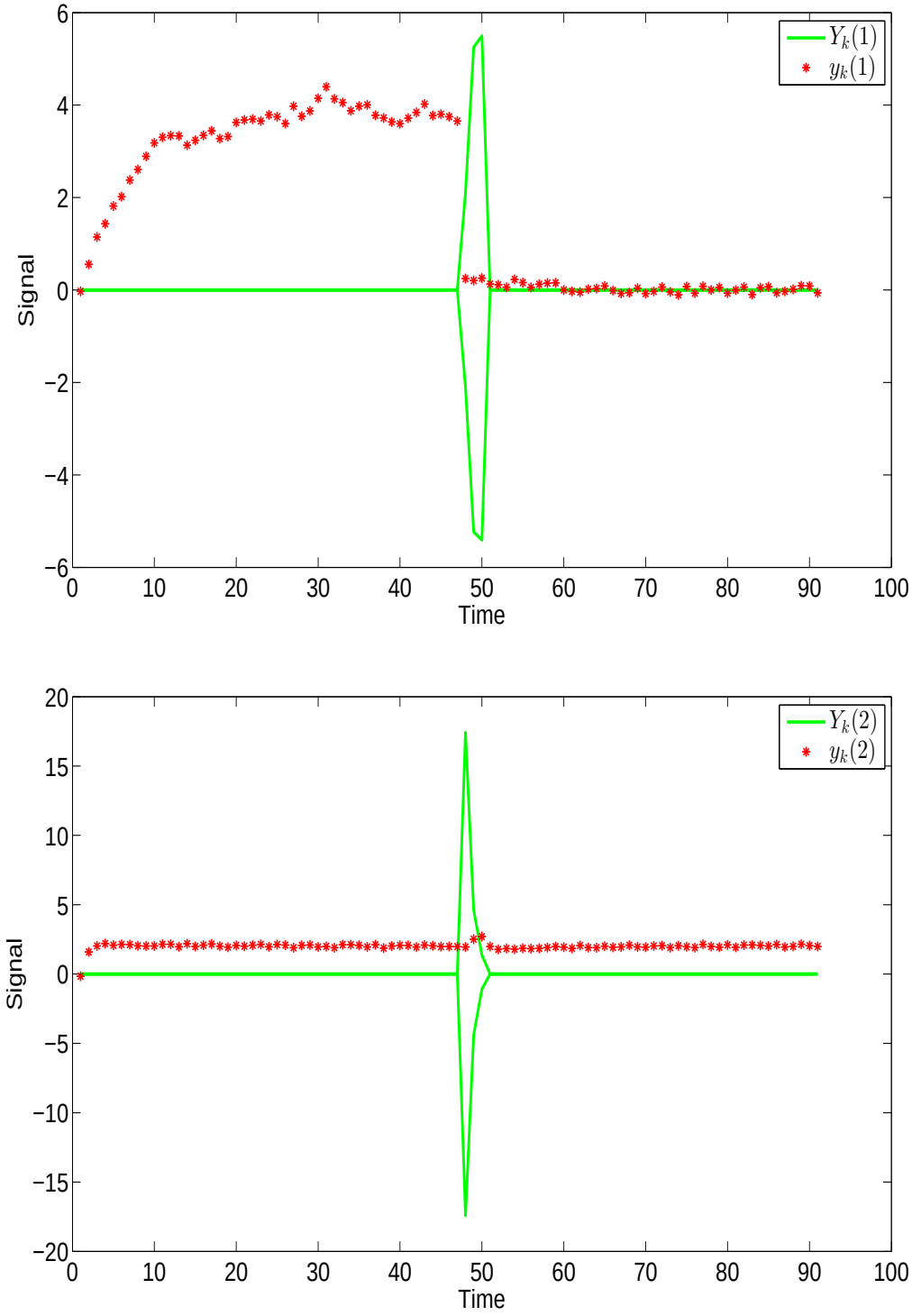


Figure 7.5: FI of Fault 1

Thus, for the three considered sensor modes (health, fault in the first sensor and fault in the second sensor), three corresponding interval observers are designed as in (7.4). Furthermore, corresponding to $u_k \in U_f$ and $\omega_k \in W$, the output sets for guaranteed FI conditions in Proposition 7.1 can be constructed, which are presented in Figure 7.3. In Figure 7.3, it can be observed that two interval components of Y_f are disjoint from those of Y_f^0, respectively, which means that the considered sensor faults can be isolated after they are detected. In the proposed scheme, there are several important state sets (i.e., X, X_M, X_{M_f}, $\bar{X}$ and $\bar{X}_f$), where X, $\bar{X}$ and X_M, and X, $\bar{X}_f$ and X_{M_f} are respectively shown in the first and second plots of Figure 7.2.

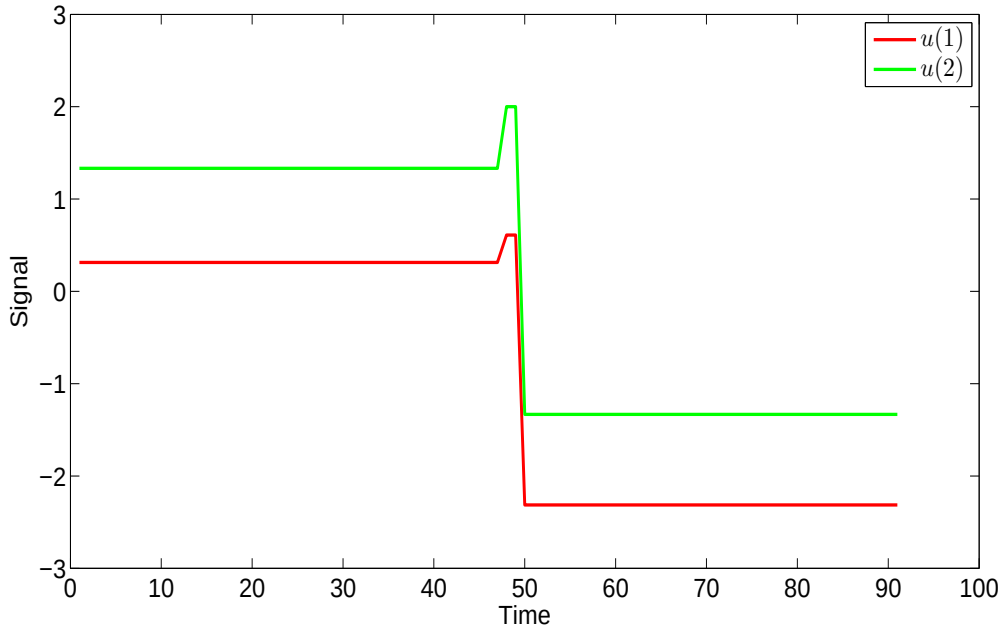


Figure 7.6: Inputs of Scenario 1

In this simulation, one defines two different scenarios for both faults, separately. The two scenarios for both faults are: from time instants 1 to 45, the plant is healthy, while from time instants 46 to 90, a sensor fault occurs in the system.

The FD and FI results of the first sensor fault are shown in Figures 7.4 and 7.5, respectively. In Figure 7.4, it is shown that a fault is detected at time instant 48, i.e., $\mathbf{0} \notin R_{48}^0$. Thus, the active FI process is started at time instant 48, i.e., (7.13) is initialized and (7.15) is tested in real time for FI (see Figure 7.5). It is shown that, at time instant 50, the first component of y_k respects its bound $Y_k(1)$, i.e., $y_{50}(1) \in Y_{50}(1)$, while the second component violates its bound, i.e., $y_{50}(2) \notin Y_{50}(2)$, which indicates that the first sensor fault is isolated. Thus, the first state-input setpoint pair and the corresponding interval observer should be used to reconfigure the system at time instant 50.

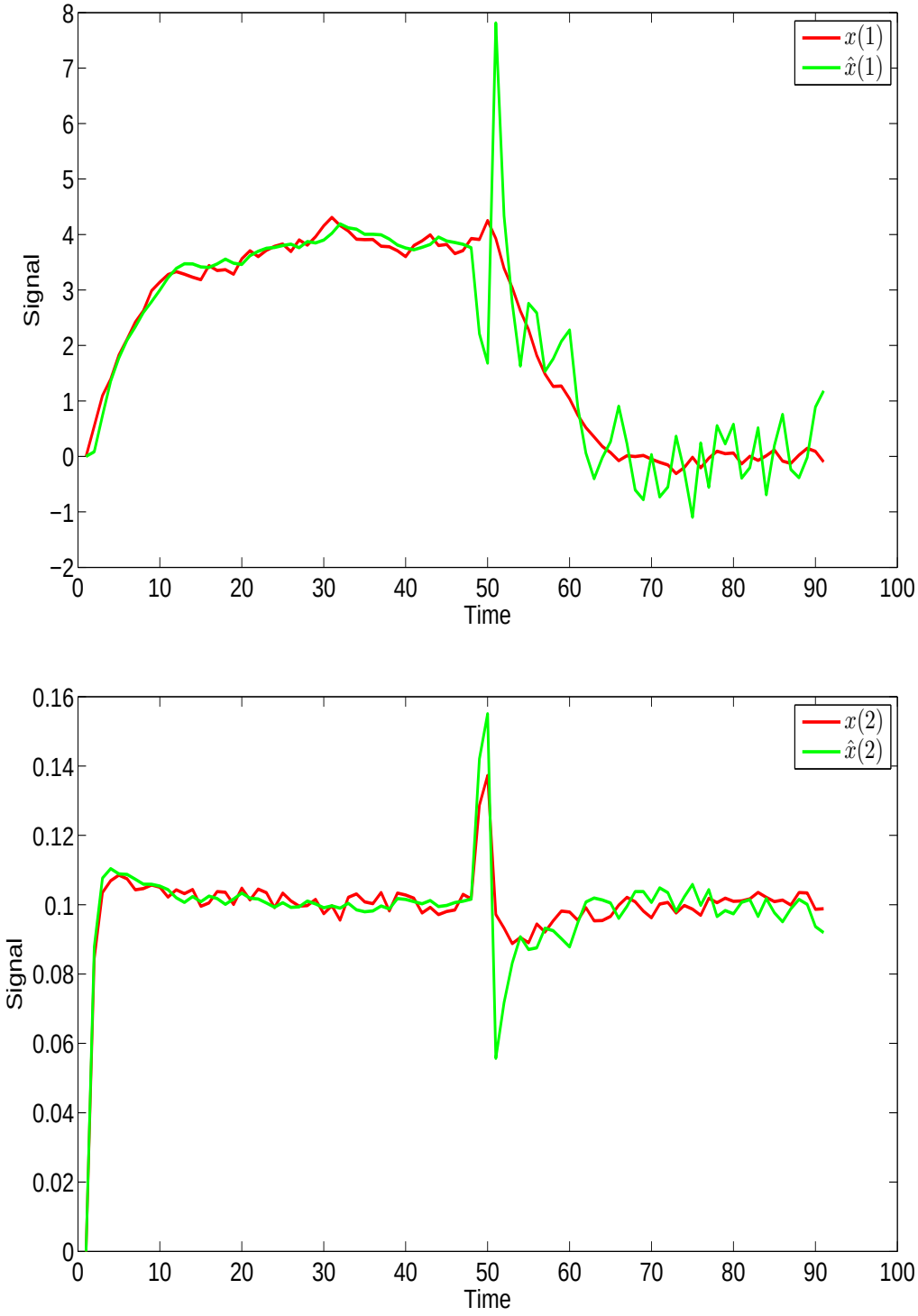


Figure 7.7: Comparison of states and state estimations of Fault 1

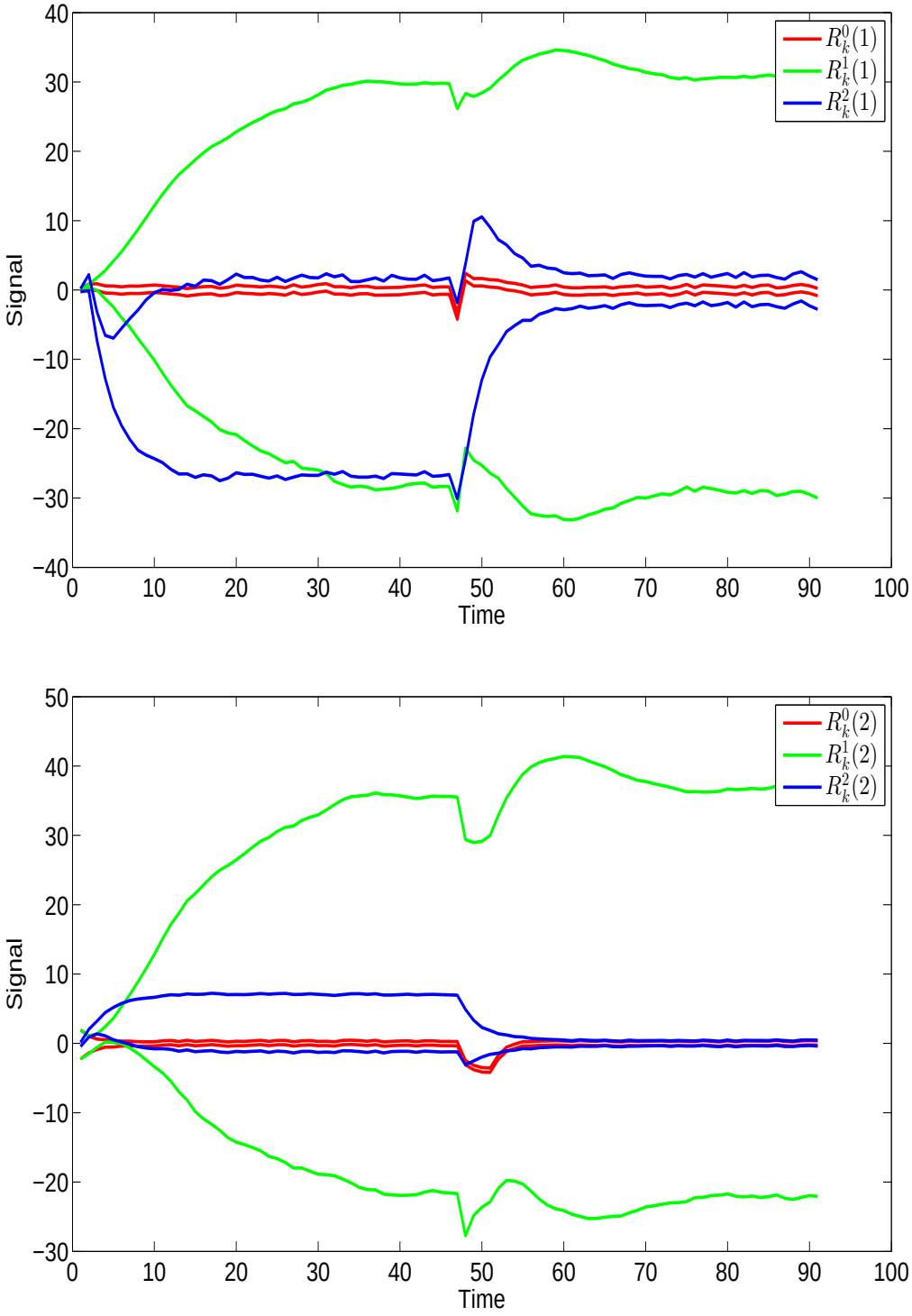


Figure 7.8: FD of Fault 2

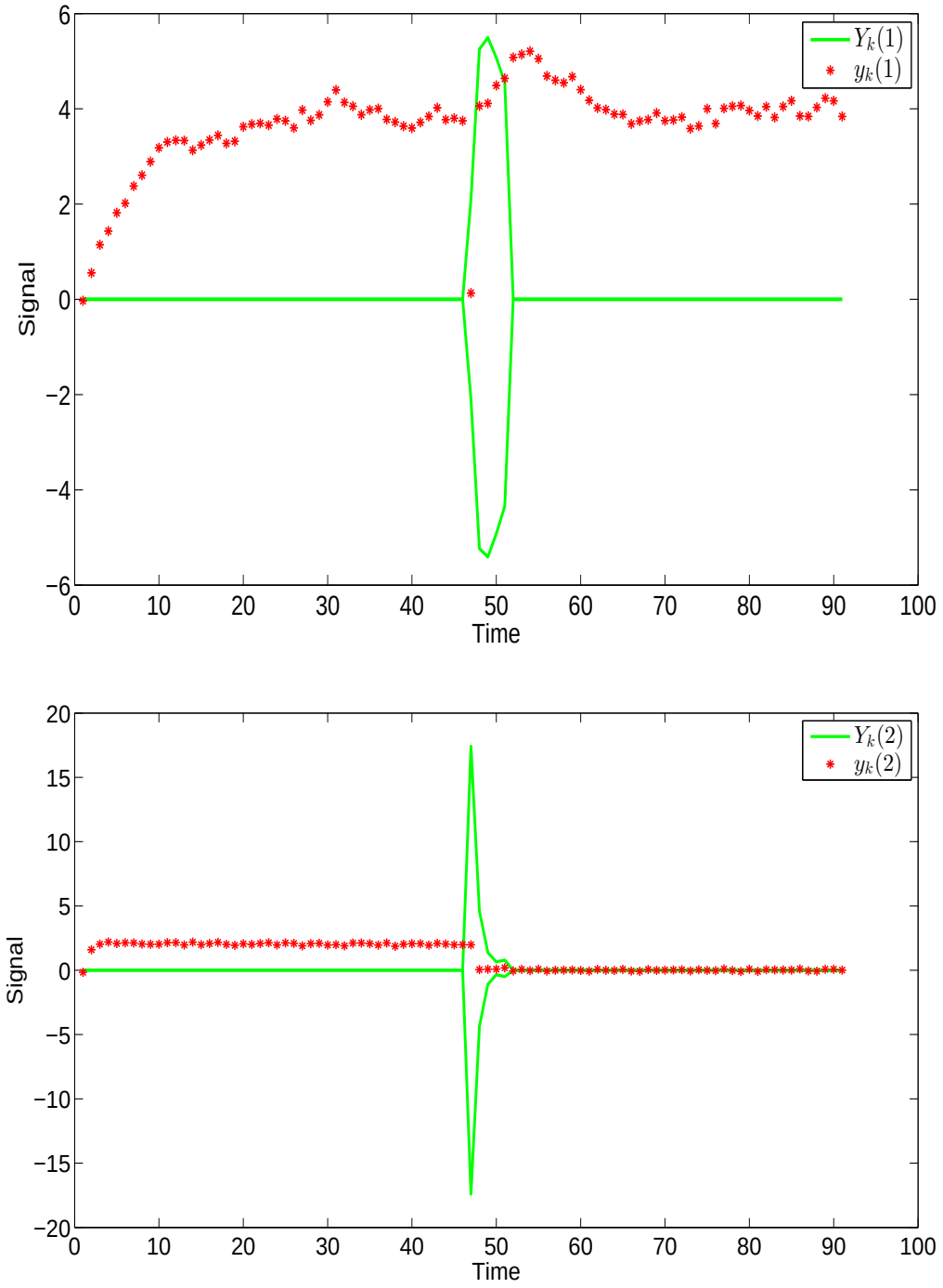


Figure 7.9: FI of Fault 2

Remark 7.12. *In the figures, $R_k^i(1)$ and $R_k^i(2)$ denote the first and second components of R_k^i from the i-th interval observer at time instant k, respectively. For the other notations in the figures, the meanings are explained in the same way.*

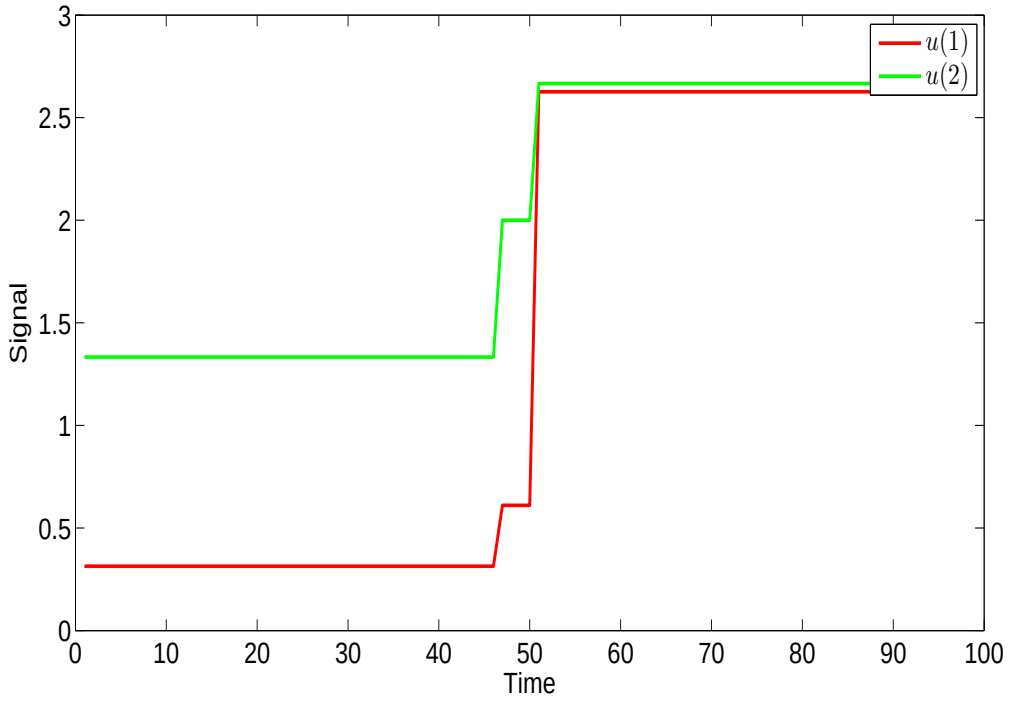


Figure 7.10: Inputs of Scenario 2

The outputs are shown in Figure 7.5 as the red stars. It can be observed that, before the first fault, the expected output y_0^* is well tracked, while after the first fault, the tracking performance becomes poor until the time instant 50 when the system is reconfigured. After the time instant 50, it can be observed that the expected y_1^* can be well tracked again.

The generated control actions corresponding to the first scenario are presented in Figure 7.6, where before fault occurrence, the control inputs satisfy the constraints. During the active FI process, because of the strategy (7.22) for feasibility guarantees, the generated inputs are constant, i.e., a step signal, which satisfy the constraint U_f. After system reconfiguration, the control inputs to tolerate the first fault are generated, which also satisfy the constraint U.

Besides, in order to show the effectiveness of state estimations (7.19), a comparison between the real states and their estimations is shown in Figure 7.7. It can be observed that (7.19) can give satisfactory state estimations in steady state.

Similarly, the FD and FI simulation results of the second fault are shown in Figures 7.8 and 7.9, respectively. In Figure 7.8, it is shown that a fault is detected at time instant 47. In

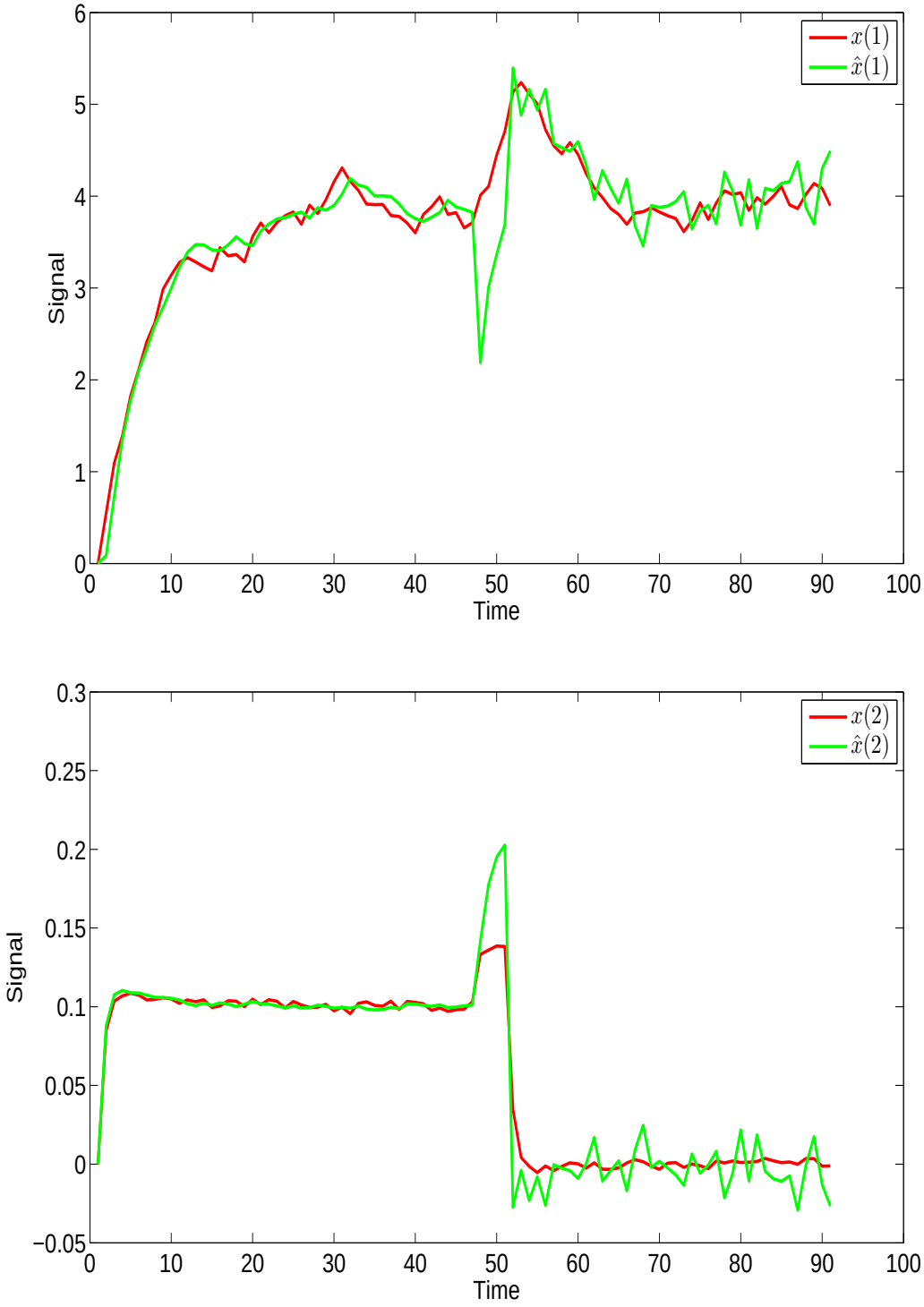


Figure 7.11: Comparison of states and state estimations of Fault 2

Figure 7.9, it is shown that the second sensor fault is isolated at time instant time instant 51 and simultaneously the controller is reconfigured with the second state-input pair and the second interval observer for the second scenario.

Similarly, the outputs are shown in Figure 7.9 as the red stars, where y_0^* and y_2^* are well tracked before the second fault and after reconfiguration, respectively. The generated control inputs for the second scenario are shown in Figure 7.10, which presents that the input constraints are always satisfied. In Figure 7.10, during active FI, it can be observed that only five control actions are generated and only five steps are needed to isolate the second fault. In Figure 7.11, a comparison between the real states and their estimations is shown. Thus, generally speaking, according to the results, it is shown that the proposed sensor FTC scheme can effectively tolerate the effect of sensor faults.

7.6 Summary

In this chapter, a sensor FTMPC scheme using min-max MPC and interval observers is proposed. By combining min-max MPC with active FI, sensor FDI and guaranteed FI conditions can be simplified. Additionally, the author proposed a novel state-estimation approach to guarantee recursive feasibility of the MPC controller. But, for RPI set construction and constraint satisfaction, the FTMPC scheme has to work under Assumptions 7.2, 7.6 and 7.7. If better methods can be proposed to deal with these issues, the performance of the sensor FTC scheme is possible to be improved.

Part IV

Concluding Remarks

Chapter 8

Conclusions and Future Research

This chapter summarizes the dissertation and gives remarks for the future research from the viewpoint of the author. The concluding remarks include two aspects. First, the main contributions and conclusions of this dissertation will be recapitulated. Second, general remarks of the entire research will be made and the future research of this topic will be discussed.

8.1 Main Conclusions

The main objective of this dissertation is to propose FTMPC schemes using set-based FDI. By using set-based FDI, one can obtain robust FDI, which is important for fault-tolerance of the system with uncertainties. With MPC techniques, the proposed fault-tolerant schemes can have ability to obtain some performance that other control strategies are difficult to reach, such as system constraint handling and active FI.

In this dissertation, one proposed new set-based FDI approaches to balance the advantages and disadvantages of the existing set-based fault diagnosis approaches. For FTC, one considered robust MPC techniques (tube-based and min-max), either of which has its own merits and drawbacks for the proposed FTC schemes. The merits and drawbacks have been discussed in the contents of this dissertation. Thus, for different requirements, different robust MPC techniques should be chosen.

This research mainly focuses on actuator and sensor FDI and FTC, which more frequently appears in actual systems. Considering different characteristics of actuator and sensor faults, actuator and sensor FDI and FTC approaches are proposed, separately. For the set-based FDI approaches, the conservatism is mainly originated from guaranteed FDI (or FI) conditions. In order to reduce this conservatism, different from the passive fault diagnosis approaches, one uses the MPC techniques to implement active FI. The proposed active FI approaches are based on MPC controllers, which are implemented by exciting the system with especially chosen inputs to obtain useful system information for FI. Generally, the system information obtained by the active approaches is ampler than that from the passive monitoring of the system.

In the proposed schemes, one only considers uncertainties from process disturbances and measurement noises. In principle, the proposed approaches can also be extended to the system with parametric uncertainties. In addition, Chapters 5 and 6 only consider faults with known magnitudes while Chapters 4 and 7 consider faults with unknown but bounded magnitudes. It is known that the latter is more realistic for applications. However, in principle, the proposed approaches in Chapters 5 and 6 can also be extended to the case of unknown but bounded faults. Besides, one gives several remarks on the aforementioned diagnosis approaches.

- For the mentioned set-based fault diagnosis approaches, the invariant set-based approach has the simplest principle, which only needs to test whether or not the residual is inside its healthy or faulty sets. Its main drawback consists in conservatism of its FDI conditions and its extension to the system with uncertainties. This extension is still not done from the current knowledge of the author. Thus, for applications that have linear time-invariant dynamics, require less computational complexity and satisfy set-separation FDI conditions, the invariant set-based approach can be used.

- For the interval observer-based approach, there already exist considerable research results. For applications such as the system with parametric uncertainties, this approach has more knowledge to refer to. Besides, this approach can obtain less conservative FDI conditions with the help of other techniques. The drawback of interval observers is its relatively high computational complexity. Moreover, it can provide robust state estimation. Thus, from the control point of view, it is beneficial for control design.

- For the set-membership approach, it can provide robust state estimation for control design. But, for general applications of diagnosis, comparing with the other two approaches, its advantages cannot be clearly observed from both computational and practical points of view. However, the set-valued observers have the simplest structure. Because, for considering actuator/sensor faults, one does not need to design the same number of observers with the considered actuator/sensor modes to monitor the system. Instead, one only needs to design one set-valued observer with adjusting the state dynamics (actuator modes)/measurement equations (sensor modes) corresponding to the current system mode.

In addition, one also makes a short summary of the contributions of this dissertation for the sake of making the motivation and contributions of this research more easily understand, where the main contributions are presented as follows:

- The relationship between invariant sets and interval observers in FD is briefly investigated in this dissertation, which gives the advantages and disadvantages of the two approaches. This investigation is the research basis of this dissertation.

- By using invariant sets, one proposed several different FDI approaches based on interval observers. Specially for FI, invariant sets are used to establish FDI (or FI conditions), which extends interval observers from the FD to FI applications.

- For FDI and FTC frameworks based on a bank of observers, this dissertation proposed approaches that make full use of the available information from all observers. Based on these information, a strategy proposed in Chapter 5 is used to reduce the complexity of the FDI approach by removing unnecessary/redundant system-operating information from all observers.
- By utilizing robust MPC techniques, one can manipulate the bound of inputs of the plant directly (i.e., min-max MPC) or indirectly (i.e., tube-based MPC) to actively isolate faults. The proposed active FI approach can obtain extra system information for FI that the passive fault diagnosis approaches cannot obtain, which can effectively reduce the conservatism of the set-based approaches.
- Taking differences of characteristics of actuator and sensor faults into account, FDI and FTC approaches are proposed for actuator and sensor faults, respectively.

8.2 Future Research

In this dissertation, one has proposed different strategies to make full use of all available system information for FDI. For example, by using the system-operating information from all observers, one can loosen guaranteed FDI conditions and by proposing the MPC-based active FI approaches, one can reduce conservatism in comparison with the passive approach. However, one cannot say that the proposed approaches have already been perfect. For the author, considering the practical values of MPC and set-based FDI, the main objective is to propose several FTMPC frameworks with the MPC techniques and the set-based FDI approaches. In these FTMPC schemes, there are still unperfect aspects that should be further improved. In the following, one summarizes the points that have space to be enhanced.

- The extensions of all the proposed approaches to the system with parametric uncertainties, the faults unknown but bounded and the system with more complex dynamics such as non-linearity.
- For the proposed FTMPC scheme in Chapter 6, a key point is to assure that the system constraints are always satisfied. But, during active FI, it is difficult for the proposed approach to always guarantee constraint satisfaction. Thus, it is necessary to propose a strategy to cope with this problem and improve the proposed scheme.
- Since the min-max MPC technique can directly manipulate the size of input sets of the plant, it is chosen as the control strategy of the proposed FTMPC scheme in Chapter 7. But its drawback consists in its computational complexity. Thus, in principle, any method that can reduce computational complexity of the min-max MPC technique can be used to enhance the scheme. Additionally, if better state estimation and constraint satisfaction strategies can be proposed, the FMPC scheme can also be further improved.
- The proposed FTMPC schemes are implemented by switching input constraint sets of the MPC controllers to force that the generated inputs injected into the plant can establish

guaranteed FI conditions on-line. Thus, it is necessary to give a systematic approach for the design of input sets for the proposed active FI strategy.

- In this dissertation, for different fault types and diagnosis requirements, one proposed different FDI and FTC approaches. But, an important fundamental problem is how to compute all magnitudes of faults that are detectable and isolable by the set-based passive and active FDI approaches.
- Despite this dissertation has proposed different FDI and FTC approaches and different applications have be done with these approaches, they are not applied into real systems because of time. Thus, an interesting direction is to apply these FDI and FTC approaches into real case studies.

Bibliography

[1] M. Abdel-Geliel, E. Badreddin, and A. Gambier. Application of model predictive control for fault tolerant system using dynamic safety margin. In *Proceedings of the 2006 American Control Conference*, Minneapolis, Minnesota, USA, June 2006. 2.1.3

[2] T. Alamo, J.M. Bravo, and E.F. Camacho. Guaranteed state estimation by zonotopes. *Automatica*, 41(6):1035–1043, 2005. 1.1, 2.1.2, 2.2.1.2, 2.2.1.2, 4.6, 5.19

[3] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747 – 1767, 1999. 1.1

[4] F. Blanchini and S. Miani. *Set-theoretic Methods in Control*. Birkhäuser Boston, 2008. 2.2.1.1

[5] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag, Berlin, Germany, 2006. 1.1, 2.1.1, 1

[6] M. Blanke, M. Staroswiecki, and N. E. Wu. Concepts and methods in fault-tolerant control. In *Proceedings of the 2001 American Control Conference*, Virginia, USA, June 2001. 1.1

[7] J. Blesa, V. Puig, J. Romera, and J. Saludes. Fault diagnosis of wind turbines using a set-membership approach. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 28 August - 2 September 2011. 1.1, 1.2, 2.1.2

[8] F. Borrelli, A. Bemporad, and M. Morari. *Predictive Control for Linear and Hybrid Systems*. Model Predictive Control Lab, UC-Berkeley, USA, 2014. 1.1, 2.2.1.1, 2.2.2.2, 2.2.3.1

[9] J.D. Bošković and R.K. Mehra. Fault accommodation using model predictive methods. In *Proceedings of the 2002 American Control Conference*, Anchorage, AK, USA, May 2002. 2.1.3

[10] E.M. Bronstein. Approximation of convex sets by polytopes. *Journal of Mathematical Sciences*, 153(6):727 – 762, 2008. 2.2.1.1

[11] E.F. Camacho, T. Alamo, and D. Muñoz la Pena. Fault-tolerant model predictive control. In *Proceedings of 15th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2010*, Bilbao, Spain, September 2010. 2.1.3

[12] E.F. Camacho and C. Bordons. *Model Predictive Control*. Springer-Verlag, Berlin, Germany, 2004. 1.1

[13] W. Chai and J. Qiao. Passive robust fault detection using RBF neural modeling based on set membership identification. *Engineering Applications of Artificial Intelligence*, 28(0):1 – 12, 2014. 2.1.2

[14] J. Chen, R. J. Patton, and H. Zhang. Design of unknown input observers and robust fault detection filters. *International Journal of Control*, 63(1):85–105, 1996. 2.1.2

[15] C. Combastel. A state bounding observer based on zonotopes. In *Proceedings of the 2003 European Control Conference*, Cambridge, UK, 2003. 2.1.2, 2.2.1.2

[16] F.A. de Almeida and D. Leissling. Fault-tolerant flight control system using model predictive control. In *Proceedings of the 2009 Brazilian Symposium on Aerospace Eng.& Applications*, São Paulo, Brazil, September 2009. 2.1.3

[17] G. Franzè, F. Tedesco, and D. Famularo. Actuator fault tolerant control: a set-theoretic approach. In *In proceedings of the 51st IEEE Conference on Decesion and Control*, December 2011. 2.1.2

[18] J.L. Gouzé, A. Rapaport, and M.Z. Hadj-Sadok. Interval observers for uncertain biological systems. *Ecological Modelling*, 133:45 – 56, 2000. 1.1, 2.1.2, 3.3

[19] P. Guerra and V. Puig. Passive robust fault detection using interval MA parity equations: Inverse vs direct image tests. In *Proceedings of the 17th IFAC World Congress*, Seoul, South Korea, July 2008. 1.1

[20] P. Guerra, V. Puig, and M. Witczak. Robust fault detection with unknown-input interval observers using zonotopes. In *Proceedings of the 17th IFAC World Congress*, Seoul, South Korea, July 2008. 1.1, 1.2, 2.1.2, 3.3, 4.1

[21] J. Jiang. Fault-tolerant control systems - an introductory overview 1. *Automatica*, 31(1):161–174, 2005. 2.1.1

[22] D.A. Joosten, T.J.J. van den Boom, and T.J.J. Lombaerts. Fault-tolerant control using dynamic inversion and model-predictive control applied to an aerospace benchmark. In *Proceedings of the 17th IFAC World Congress*, Seoul, South Korea, July 2008. 2.1.3

[23] W. K*ü*hn. Rigorously computed orbits of dynamical systems without the wrapping effect. *Computing*, 61(1), 1998. 2.2.1.2

[24] M. Kettunen and S-L. Jämsä-Jounela. Fault tolerant MPC with an embedded FDI system. In *Proceedings of the 1st IFAC Workshop on Applications of Large Scale Industrial Systems*, Helsinki, Finland, August 2006. 2.1.3

[25] E. Kofman, H. Haimovich, and M.M. Seron. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control*, 80(2):167–178, 2007. 2.2.2.1, 3.2

[26] I. Kolmanovsky and E. Gilbert. Theory and computation of disturbance invariant sets for discrete-time linear systems. *Mathematical Problems in Engineering*, 4:317–367, 1998. 1.1

[27] K.I. Kouramas, S.V. Raković, E.C. Kerrigan, J. Allwright, and D.Q. Mayne. On the minimal robust positively invariant set for linear difference inclusions. In *Proceedings of the 44th IEEE Conference on Decision and Control and the 2005 European Control Conference*, Seville, Spain, December 2005. 1.1

[28] J. Löfberg. *Min-max Approaches to Robust Model Predictive Control*. PhD thesis, Department of Electrical Engineering, Linköping University, Sweden, 2003. 1.1, 2.2.3.3

[29] V.T.H. Le, T. Alamo, E.F. Camacho, C.N. Stoica, and D. Dumur. A new approach for guaranteed state estimation by zonotopes. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 28 August - 2 September 2011. 2.1.2

[30] V.T.H. Le, C.N. Stoica, T. Alamo, E.F. Camacho, and D. Dumur. Zonotope-based set-membership estimation for multi-output uncertain systems. In *Proceedings of 2013 IEEE international Symposium on Intelligent Control (ISIC), Part of 2013 IEEE Multi-Conference on Systems and Control*, Hyderabad, India, August 2013. 2.2.1.2

[31] J.M. Maciejowski. Modelling and predictive control: Enabling technologies for reconfiguration. *Annual Reviews in Control*, 23(0):13 – 23, 1999. 1.1, 2.1.3

[32] J.M. Maciejowski. *Predictive Control with Constraints*. Prentice Hall, 2002. 1.1, 2.2.3.1

[33] J.M. Maciejowski and C.N. Jones. MPC fault-tolerant flight control case study: Flight 1862. In *Proceedings of the 5th IFAC Symposium SAFEPROCESS-2003: Fault Detection, Supervision and Safety for Technical Processes*, Washington, USA, August 2003. 2.1.3

[34] M.R. Mallick and S.A. Imtiaz. A MPC based fault tolerant control strategy for actuator fault. In *Proceedings of the 2011 International Conference on Electrical and Control Engineering (ICECE)*, Yichang, China, September 2011. 2.1.3

[35] D.Q. Mayne, S.V. Raković, R. Findeisen, and F. Allgöwer. Robust output feedback model predictive control of constrained linear systems. *Automatica*, 42(7):1217 – 1222, 2006. 1.1, 2.2.3.2, 2.5, 6.2.4, 6.4.1, 6.4.1

[36] F. Mazenc and O. Bernard. Interval observers for linear time-invariant systems with disturbances. *Automatica*, 47(1):140 – 147, 2011. 2.1.2, 3.3, 4.1

[37] L.F. Mendonca, S.M. Vieira, J.M.C. Sousa, and J.M.G. da Costa. Fault accommodation using fuzzy predictive control. In *Proceedings of the 2006 IEEE International Conference on Fuzzy Systems*, Vancouver, BC, Canada, July 2006. 2.1.3

[38] P.H. Menold, F. Allgöwer, and R.K. Pearson. Nonlinear structure identification of chemical processes. *Computers & Chemical Engineering*, 21(0):S137 – S142, 1997. 4.6

[39] J. Meseguer, V. Puig, and T. Escobet. Robust fault detection linear interval observers avoiding the wrapping effect. In *Proceedings of the 17th World Congress*, Seoul, South Korea, July 2008. 1.2, 2.1.2, 3.3, 3.3, 4.1

[40] J. Meseguer, V. Puig, T. Escobet, and R. Sarrate. Observer gain effect in linear interval observer-based fault detection. In *Proceedings of the 46th IEEE Conference on Decision and Control*, New Orleans, Louisiana, USA, December 2007. 2.1.2, 3.2, 3.3

[41] C. Ocampo-Martinez, J.A. De Doná, and M.M Seron. Actuator fault-tolerant control based on set separation. *International Journal of Adaptive Control and Signal Processing*, 24(12):1070– 1090, 2010. 2.1.2, 3.2, 6.5, 6.5, 7.5

[42] C. Ocampo-Martinez, V. Puig, J. Quevedo, and A. Ingimundarson. Fault tolerant model predictive control applied on the Barcelona sewer network". In *Proceedings of the 44th IEEE Conference on Decision and Control and the 2005 European Control Conference*, Seville, Spain, December 2005. 2.1.3

[43] P.F. Odgaard, J. Stoustrup, and M. Kinnaert. Fault tolerant control of wind turbines-a benchmark model. In *Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Process*, Barcelona, Spain, July 2009. 5.6

[44] S. Olaru, J.A. De Doná, M.M. Seron, and F. Stoican. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12):2622–2640, 2010. 2.1.2, 2.2.2.1, 3.2, 3.2, 3.5.2

[45] R.J. Patton and J. Chen. Observer-based fault detection and isolation: Robustness and applications. *Control Engineering Practice*, 5(5):671 – 682, 1997. 2.1.2

[46] V. Puig. Fault diagnosis and fault tolerant control using set-membership approaches: Application to real case studies. *International Journal of Applied Mathematics and Computer Science*, 20(4):619–635, 2010. 2.1.2

[47] V. Puig, J. Quevedo, T. Escobet, and S. de las Heras. Passive robust fault detection approaches using interval models. In *Proceedings of the 15th IFAC World Congress*, Barcelona, Spain, July 2002. 1.1, 1.2, 2.1.2, 2.2.1.2, 3.3

[48] V. Puig, J. Quevedo, T. Escobet, and A. Stancu. Passive robust fault detection using linear interval observers. In *Proceedings of the 5th IFAC Symposium SAFEPROCESS-2003: Fault Detection, Supervision and Safety for Technical Processes*, Washington, USA, August 2003. 1.1, 2.1.2, 2.2.1.2

[49] V. Puig, A. Stancu, and J. Quevedo. Observers for interval systems using set and trajectory-based approaches. In *Proceedings of the 44th IEEE Conference on Decision and Control and the 2005 European Control Conference*, Seville, Spain, December 2005. 2.1.2, 3.3, 3.5.1

[50] D.M. Raimondo, R.D. Braatz, and J.K. Scott. Active fault diagnosis using moving horizon input design. In *Proceedings of 2013 European Control Conference (ECC)*, Zürich, Switzerland, July 17-19 2013. 2.1.3

[51] D.M. Raimondo, G. Roberto Marseglia, R.D. Braatz, and J.K. Scott. Fault-tolerant model predictive control with active fault isolation. In *Proceedings of 2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, Nice, France, October 9-11 2013. 2.1.3, 6.1

[52] T. Raïssi, G. Videau, and A. Zolghadri. Interval observer design for consistency checks of nonlinear continuous-time systems. *Automatica*, 46(3):518 – 527, 2010. 2.1.2, 3.3

[53] S.V. Raković, E.C. Kerrigan, K.I. Kouramas, and D.Q. Mayne. Invariant approximations of the minimal robust positively invariant set. *IEEE Transactions on Automatic Control*, 50(3):406 – 410, March 2005. 1.1

[54] P. Rosa. *Multiple-Model Adaptive Control of Uncertain LPV Systems*. PhD thesis, Electrical and Computer Engineering, Instituto Superior Técnico, Portugal, 2011. 2.1.2, 2.1.3

[55] M.M. Seron and J.A. De Doná. Actuator fault tolerant multi-controller scheme using set separation based diagnosis. *International Journal of Control*, 83(11):2328–2339, 2010. 2.1.2, 3.2

[56] M.M. Seron, J.A. De Doná, and J.J. Martinez. Invariant set approach to actuator fault tolerant control. In *Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Barcelona, Spain, 30 June - 3 July 2009. 2.1.2

[57] M.M. Seron, J.A. De Doná, and S. Olaru. Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions. *IEEE Transactions on Automatic Control*, 57(7):1657–1669, 2012. 2.1.2, 3.2

[58] M.M. Seron, X.W. Zhuo, J.A. De Doná, and J.J. Martínez. Multisensor switching control strategy with fault tolerance guarantees. *Automatica*, 44(1):88–97, 2008. 2.1.2, 3.2, 5.1

[59] R.C. Shekhar and J.M. Maciejowski. Robust predictive control with feasible contingencies for fault tolerance. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 28 August-2 September 2011. 2.1.3

[60] F. Stoican. *Fault tolerant control based on set-theoretic methods*. PhD thesis, E3S-Supelec systems Science, Automatic Control Department, Supélec, France, October 2011. 2.1.2

[61] F. Stoican, C.F. Raduinea, and S. Olaru. Adaptation of set theoretic methods to the fault detection of a wind turbine benchmark. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 28 August-2 September 2011. 5.6

[62] F. Stoican, M.M. Seron S. Olaru, and J.A. De Doná. Reference governor design for tracking problems with fault detection guarantees. *Journal of Process Control*, 22(5):829 – 836, 2012. 2.1.2

[63] S. Sun, L. Dong, L. Li, and S. Gu. Fault-tolerant control for constrained linear systems based on MPC and FDI. *International Journal of Information and Systems Sciences*, 4(4):512 –23, 2008. 2.1.2, 2.1.3

[64] R. Wang. *Fault-Tolerant Control and Fault-Diagnosis Design for Over-Actuated Systems with Applications to Electric Ground Vehicles*. PhD thesis, Department of Mechanical and Aerospace Engineering, The Ohio State University, USA, 2013. 2.1.3

[65] F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Actuator-fault detection and isolation based on interval observers and invariant sets. In *Proceedings of the 52nd IEEE Conference on Decision and Control*, Florence, Italy, December 10-13 2013. 4.1, 5.1

[66] F. Xu, V. Puig, C. Ocampo-Martinez, F. Stoican, and S. Olaru. Improved fault detection and isolation strategy using a bank of interval observers. In *Proceedings of the 19th IFAC World Congress*, Cape Town, South Africa, August 24 - 29 2014. 5.1

[67] F. Xu, F. Stoican, V. Puig, C. Ocampo-Martinez, and S. Olaru. Fault detection and isolation based on the combination of a bank of interval observers and invariant sets. In *Proceedings of the 21st Mediterranean Conference on Control and Automation*, Chania, Greece, June 25 - 28 2013. 4.1, 4.5.1, 4.5.1, 5.1

[68] F. Xu, F. Stoican, V. Puig, C. Ocampo-Martinez, and S. Olaru. On the relationship between interval observers and invariant sets in fault detection. In *Proceedings of the 2nd International Conference on Control and Fault-Tolerant Systems*, Nice, France, October 9 - 11 2013. 3.4

[69] X. Yang and J.M. Maciejowski. Fault-tolerant model predictive control of a wind turbine benchmark. In *Proceedings of the 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Mexico City, Mexico, August 2012. 2.1.3

[70] A. Yetendje, M. M. Seron, and J. A. De Doná. Robust MPC design for fault tolerance of constrained multisensor linear systems. In *Proceedings of the 2010 International Conference on Control and Fault-Tolerant Systems*, Nice, France, October 6 - 8 2010. 2.1.3, 7.1

[71] A. Yetendje, M.M. Seron, and J.A. De Doná. Robust multiactuator fault-tolerant MPC design for constrained systems. *International Journal of Robust and Nonlinear Control*, 23(16):1828‘C1845, 2013. 2.1.3, 6.1

[72] Y.M. Zhang and J. Jiang. Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, 32(2):229 – 252, 2008. 2.1.1

[73] G.M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics, Springer-Verlag, Berlin, Germany, 1994. 2.2