

FAULT TOLERANT CONTROL SYSTEMS DESIGN

by

Qing Zhao

Department of Electrical and Computer Engineering
Faculty of Engineering Science

Submitted in partial fulfilment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Graduate Studies
The University of Western Ontario
London, Ontario

August 1999

© Qing Zhao 1999



National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-42559-2

Canada

ABSTRACT

In this thesis, the design of a new class of control systems, called Fault Tolerant Control Systems (FTCS), has been studied thoroughly. Fault Tolerant Control Systems are closed-loop control systems which can tolerate system component faults or failures and maintain the system stability and a certain degree of performance. FTCS are extremely important in safety-critical applications. In this thesis, the system model with component faults is first formulated mathematically. Important issues in FTCS, such as redundancy, performance degradation, and time constraints are explored in depth. The definitions of actuator and sensor redundancy are first introduced and then clearly elaborated. Based on how the system redundancy is utilized, FTCS can be classified into active FTCS and passive FTCS. With a better understanding of the characteristics of both types of FTCS, the problems of designing such systems are investigated in a unified framework. Existing design methodologies are reviewed. New design approaches for passive FTCS protecting against actuator/sensor failures are proposed. The proposed methods have effectively utilized actuator redundancy and sensor redundancy in the design to achieve the fault tolerance. For active Fault Tolerant Control Systems, Fault Detection and Identification (FDI) schemes are introduced first and two common design techniques based on state estimation and parameter estimation are compared. The comparison is mainly based on the fault detection rate and availability of the fault information. By taking into account the integration of FDI and reconfigurable control, a new bounding parameter estimation based fault identification scheme is proposed followed by an applicable reconfigurable control scheme. The integrated design of FDI and reconfigurable control is thus achieved. Three design examples are presented to demonstrate the effectiveness of the proposed design methods for both passive and active FTCS. The main contribution of this thesis is that new design methodologies for both passive and active FTCS are developed, the important concept of system redundancy are incorporated in the proposed design. In addition, many important issues of FTCS are first explored in this thesis.

Keywords: Redundancy, Reliability, Fault Tolerant Control Systems (FTCS), Fault Detection and Identification (FDI), Reconfigurable control

“In building complex computing machines, unreliability of components should be overcome not by making the components more reliable, but by organizing them in such a way that the reliability of the whole computer is greater than the reliability of its parts.”

----- von Neumann, 1956

CO-AUTHORSHIP

The following thesis contains material from previously published manuscripts, manuscripts submitted for publication, and manuscripts in preparation for publication, co-authored by Qing Zhao and Jin Jiang.

All the research, including developmental, simulation and experimental work presented in this thesis was performed by Qing Zhao. Original manuscripts, versions of which appear in Chapter 4-6 of this thesis, were written by Qing Zhao.

ACKNOWLEDGEMENTS

I would like to express my sincerest gratitude to my thesis advisor, Professor Jin Jiang, for his invaluable guidance, great patience and consistent encouragement during the last four years. His enthusiasm in research and teaching has profoundly influenced me. I am grateful to him for sharing his clear thinking and deep insights with me during our numerous discussions.

In addition, I am thankful to Mr. Yonghui Xu for helping me with the experiments during our collaboration. I am also grateful to Mr. Dennis Michaelson for carefully reading this manuscript and making valuable comments. His time and effort are greatly appreciated. My appreciation also goes to my friends and colleagues at University of Western Ontario for their useful advice and continuous moral support.

I am especially grateful to my sisters, my nephew, and my nieces for their love. Finally, I would like to dedicate this thesis to my dearest parents. This work might not have been possible without their consistent love, understanding and encouragement.

TABLE OF CONTENTS

	Page
Certificate of Examination.....	ii
Abstract and Keywords	iii
Co-Authorship.....	v
Acknowledgements	vi
Table of Contents	vii
List of Figures	xi
List of Notation and Symbols.....	xiv
Chapter 1 Introduction.....	1
1.1 Fault Tolerant Control Systems	1
1.2 Development of Fault Tolerant Control Systems Design Techniques ...	4
1.3 Scope of the Thesis	9
1.4 Bibliography	10
Chapter 2 Special Considerations in Fault Tolerant Control Systems.....	16
2.1 Introduction	16
2.2 Characteristics of Dynamic Systems with Faults	16
2.2.1 Faults in dynamic systems	16
2.2.2 Modelling of faults	18
2.3 Design Objectives of FTCS	29
2.4 Specifications and Performance Measures in FTCS.....	31

2.4.1	Three time periods of FTCS	31
2.4.2	Performance degradation	33
2.4.3	Performance measures for pre-fault and post-fault system operation	34
2.4.4	Performance measures for the system during faults	37
2.5	Conclusion	40
2.6	Bibliography	40
Chapter 3	Redundancies in Fault Tolerant Control Systems	41
3.1	Introduction.....	41
3.2	Classification of Redundancies	42
3.2.1	Hardware redundancies	42
3.2.2	Analytical redundancies.....	44
3.3	Representation of Redundancies.....	45
3.3.1	System structure with hardware redundancies.....	45
3.3.2	Actuator redundancy.....	47
3.3.3	Sensor redundancy	55
3.4	Conclusion	57
3.5	Bibliography	58
Chapter 4	Design of Passive Fault Tolerant Control Systems.....	59
4.1	Introduction.....	59
4.2	Review of Existing Passive FTCS Design Techniques	60
4.2.1	The concept of system integrity and related work	60
4.2.2	Methods based on decentralized/centralized control	68
4.2.3	Methods based on regional eigenvalue assignment	74
4.3	Passive FTCS Design Against Actuator Failures	78
4.3.1	Problem formulation.....	78
4.3.2	Design of the pre-compensator	82
4.3.3	Design of reliable state-feedback and the <i>PI</i> controller.....	85
4.3.4	Design examples	92
4.4	Passive FTCS Design Against Sensor Failures	109

4.4.1	Problem formulation	109
4.4.2	Design of the control system	112
4.4.3	Reliable DC drive system	114
4.5	Conclusion	123
4.6	Bibliography	124
Chapter 5	Fault Detection and Identification.....	127
5.1	Introduction	127
5.2	Principles of FDI.....	128
5.3	State Estimation Based FDI	130
5.3.1	Residual generation using observers or Kalman filters	130
5.3.2	Observer/Kalman filter based fault detection	135
5.4	Parameter Estimation Based FDI	139
5.4.1	Residual generation using parameter estimation schemes.....	139
5.4.2	RLS parameter estimation based fault detection	145
5.5	Comparison of State Estimation and Parameter Estimation Based FDI Schemes	147
5.6	A New FDI Scheme Based on a Bounding Parameter Estimation Algorithm	149
5.7	Conclusion	158
5.8	Bibliography	158
Chapter 6	Design of Reconfigurable Control Systems	160
6.1	Introduction.....	160
6.2	Review of Existing Design Techniques for Reconfigurable Control Systems	161
6.2.1	Pseudo-inverse method	161
6.2.2	Model-following method	164
6.2.3	Eigenstructure assignment method	168
6.3	Design of an Integrated FDI and Reconfigurable Control Scheme	172
6.3.1	Problem formulation	172

	6.3.2 Design of state-feedback control reconfiguration	176
6.4	Design Example: Active Fault Tolerant Control of a Lab-Scale Three-Tank System.....	184
	6.4.1 System description.....	184
	6.4.2 Experimental results	191
6.5	Conclusion	193
6.6	Bibliography	193
Chapter 7	Conclusions and Future Works	195
7.1	Conclusions	195
7.2	Future works	197
7.3	Bibliography	198
Appendix	An Algorithm to Compute the Nominal Interval Polynomial.	199
Attachment	A Copy of Copyright Release Letter	203
Vita		204

LIST OF FIGURES

	page
Chapter 2	
Figure 2.1 Component faults in a closed-loop control system.....	17
Figure 2.2 Elements in a control system.....	18
Figure 2.3 System elements in the state-space representation.....	20
Figure 2.4 Transients in a dynamic system.....	29
Figure 2.5 Objective list of FTCS.....	31
Figure 2.6 Three time periods of system operation in the presence of faults	32
Figure 2.7 Performance degradation in terms of eigenvalue locations	36
Figure 2.8 H_{∞} norm based performance measures	36
Figure 2.9 The allowable space and the trajectory of the system	39
Chapter 3	
Figure 3.1 A system with multiple actuators and multiple sensors	46
Figure 3.2 Interpretation of the uniform actuator redundancy	54
Figure 3.3 Hybrid redundant sensors	57
Chapter 4	
Figure 4.1 The reliable control system structure using LQR design	64
Figure 4.2 Centralized control with plant failures	69
Figure 4.3 Decentralized control with plant failures	69
Figure 4.4 Multiple control system with controller failures.	70
Figure 4.5 A Γ -stability region	75
Figure 4.6 Graphical interpretation of simultaneous stabilization based on regional eigenvalue assignment.....	76
Figure 4.7 An admissible region of the state-feedback gain to guarantee the system stability against sensor failure	77

Figure 4.8	The closed-loop system structure of the proposed passive FTCS against actuator failures	81
Figure 4.9	The block diagram representation of the proposed passive FTCS against actuator failures	86
Figure 4.10	The Γ -stability region used in the proposed method	88
Figure 4.11	Geometric interpretation in the parametric space.....	92
Figure 4.12	Step response of the closed-loop system in three operation modes	97
Figure 4.13	Normal operation: (a) System response; (b) Control signals from the aileron and the rudder	98
Figure 4.14	Aileron failure: (a) System response; (b) Control signals from the aileron and the rudder	98
Figure 4.15	Rudder failure: (a) System response; (b) Control signals from the aileron and the rudder	99
Figure 4.16	Dual-actuator ball-beam system	100
Figure 4.17	Kinematic relationship of the ball-beam system	101
Figure 4.18	The structure of ball-beam balance control system.....	104
Figure 4.19	Step response of the system under two motor operation	106
Figure 4.20	Step response of the system under single motor operation	107
Figure 4.21	Fault-induced transients during the operation	108
Figure 4.22	Unstable system response under single motor operation using conventional control.....	109
Figure 4.23	The illustrative diagram of the passive control system structure against sensor faults	110
Figure 4.24	Open-loop DC motor drive system with current sensor	115
Figure 4.25	Reliable servo system structure	118
Figure 4.26	Comparison of the measured and the estimated motor speed	120
Figure 4.27	The performance of FTCS and the conventional design under the 20% reduction in the sensor effectiveness	121
Figure 4.28	The performance of FTCS and the conventional design for the total loss of the tacho generator signal	122

Figure 4.29	The performance of FTCS and the conventional design for the total loss of the tacho generator signal	123
 Chapter 5		
Figure 5.1	Residual generation using an observer	130
Figure 5.2	Residual generation using parameter estimation scheme	139
Figure 5.3	The parameter membership set $S(k)$ and its ellipsoid outer bounding approximation.....	151
 Chapter 6		
Figure 6.1	Control system structure using explicit model-following method	165
Figure 6.2	A general structure of a reconfigurable control system.....	173
Figure 6.3	A lab-scale coupled tank system	185
Figure 6.4	An illustrative diagram of the three-tank system	185
Figure 6.5	The system diagram of fault tolerant three-tank control system	190
Figure 6.6	System responses under the leakage fault	191

LIST OF NOTATION AND SYMBOLS

Some symbols may have other meanings and are defined where they appear.

A	State transition matrix (or system matrix) in the state-space model.
A_o	State transition matrix of nominal system.
A_f	State transition matrix of faulty system.
ΔA	Fault-induced changes modelled in the state transition matrix.
$\hat{A}(h)$	Up-dated state transition matrix at time instant h in the fault identification process.
B	Input matrix in the state-space model.
B_o	Input (control) matrix of nominal system.
B_f	Input (control) matrix of faulty system.
ΔB	Fault-induced changes modelled in the input matrix.
C	Output (observation) matrix in the state-space model.
C_o	Output (observation) matrix of nominal system.
C_f	Output (observation) matrix of faulty system.
ΔC	Fault-induced changes modelled in the output matrix.
$e(k)$	Estimation error or innovation.
$e(k+1 k)$	<i>a priori</i> estimation error in Kalman filter.

$E(h)$:	Estimation error matrix
$E_b(h)$	Matrix that contains estimation error bounds.
f_a	Unknown constant disturbance caused by failed actuators.
f_s	Constant sensor bias caused by failed sensors.
$G(s)$	System transfer function.
I_n	$n \times n$ identity matrix.
J	A quadratic cost function.
K	State feedback gain (matrix).
h	Consecutive time instant at which control reconfiguration is executed.
k	Discrete time index.
L_a	Actuator failure representation matrix, with diagonal elements indicating the operation states of the actuators.
L_s	Sensor failure representation matrix, with diagonal elements indicating operation states of the sensors.
l_i	Binary indicator representing the operation states of control elements.
M	Measurement(sensor) matrix (for measuring system outputs).
$\tilde{M}$	Measurement (sensor) matrix (for measuring system states).
m	Number of system inputs.
n	Number of system states (the system order).
p	Number of system outputs.

q	Number of sensor outputs.
$r(k)$	Residual signal.
t	Continuous time index.
u	System input signal.
v	Measurement noise
V	System reference input.
$x(k)$	System state.
$\hat{x}(k k)$	Current state estimate in Kalman filter.
$\hat{x}(k+1 k)$	Conditional state estimate based on observations $\{y(i), i = 1, 2, \dots, k\}$ in Kalman filter.
y	System output signal.
z	Sensor output signal.
α	Forgetting factor in RLS parameter estimation.
β	Selecting factor in RLS parameter estimation.
θ_o	Parameter vector in ARMA model for nominal system.
$\Delta\theta$	Parameter vector that contains fault induced parameter changes.
$\hat{\theta}$	Estimated parameters in RLS parameter estimation scheme.
λ	Eigenvalue of the closed-loop system.
$\psi(k)$	Regression vector in ARMA model.
Σ	Covariance matrix of innovation in Kalman filter.

Introduction

1.1 Fault Tolerant Control Systems

In modern life, many devices depend on automatic control for satisfactory operation. For this purpose, conventional control theory and techniques have been fully developed within the last four decades. While for a conventional controller it has been the primary design goal to achieve system stability and performance with all components functioning normally, there is an increasing need for control systems to operate properly even under component failures. Generally speaking, most conventional control design techniques do not consider scenarios of potential system component faults. As a result, a control system designed using these techniques may achieve acceptable performance during normal operation, but can fail as a system even in the event of a minor component malfunction. Therefore, in order to improve the system's robustness against component failures, new design methodology needs to be developed. This is the Fault Tolerant Control Systems (FTCS) design technique which has attracted more and more interest and attention from both academia and industry.

Fault Tolerant Control Systems (FTCS) are closed-loop control systems which can tolerate system component faults/failures and are capable of maintaining stability and a certain degree of performance given these failures. The components can range from sensors, actuators, controllers or even some parts of the plant. Needless to say, FTCS are extremely important in safety-critical applications, such as aircraft, space vehicles, and chemical and nuclear processes, where minor failures in their control systems may lead to major disasters. FTCS design techniques are also useful in production lines or continuous manufacturing processes in which slight system malfunctions may force shut-down of the

entire process and result in a loss of revenue. From an engineering point of view, reliability requirements on the above-mentioned systems are usually very high. It is true that the overall reliability of a system, to a great extent, relies on high quality components, good engineering design and careful manufacturing. However, these steps alone may not be sufficient. Due to some special considerations and criteria in safety-critical systems, more often than not, using conventional design techniques in these applications can not guarantee a satisfactory level of reliability. By applying the FTCS technique, we can further improve the system reliability.

It is fair to say that the higher the automation level of the system, the more important FTCS techniques are. The key for FTCS techniques is to employ redundancies. One can say that a necessary condition to achieve fault tolerance is the existence of redundancy. As early as 1956, Von Neumann presented the fundamental concept of redundancy in his now celebrated work "*Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components*". Thereafter, this concept has widely been utilized in the development of fault-tolerant computing systems [1]. It should be emphasized that FTCS use the very same concept. Redundancies in the context of FTCS can be in hardware or analytic forms, such as redundant sensors/actuators, or fault detection/diagnosis schemes, respectively. The existence of such redundancy increases the degree of freedom of the control system design, but it also makes the design process more complex. Due to the feedback nature of control systems and their interactions with physical systems in real-time environment, it is not always obvious how redundancies should be utilized. From this viewpoint, the design of FTCS can be considered as the management of system redundancies.

Depending on how redundancy is being utilized, FTCS can be classified into two types: passive and active. In passive FTCS, potential system component failures are assumed known *a priori*, and all taken into consideration in the control system design stage. Once the controller design is completed, it will remain fixed. When a fault occurs during system operation, the control system can tolerate such a fault without any modifica-

tion to the control strategy. In this case, the system stability and performance can be maintained. In other words, when designing a passive fault tolerant control system, one has to make sure that it works for a set of system fault scenarios. Consequently, the designed controller is usually conservative. Furthermore, the passive fault tolerant control system can only deal with an anticipated class of system component failures. The system may not perform satisfactorily when an un-expected fault occurs.

In contrast, active FTCS react to system component failures by reconfiguring control actions so that the stability/performance of the entire system can be maintained. This approach relies on a real-time fault detection and identification (FDI) scheme to provide the most up-to-date information on the system status. Such information is then used by the controller to carry out necessary control reconfiguration. The critical criteria in any active FTCS are the time constraints - more precisely, the limited amount of time available for fault detection and identification, and control system reconfiguration. Moreover, the speed of the FDI to detect the fault, the accuracy of the identified fault information, and the robustness of the FDI to disturbances are all important issues. Once designed properly, active FTCS will be able to deal with unforeseen faults. Since active FTCS involve a significant amount of on-line detection, real-time decision-making and controller reconfiguration, the trade-off between the stability and the performance of the overall system must be carefully considered.

For any FTCS, there are two types of system performance that one has to consider: (1) the performance during normal operation, and (2) the performance under various component failures. The former is universal to any control system design, but the latter is unique to FTCS. If not dealt with properly, the component failure in the system can result in many undesirable consequences, such as loss of degree of controllability/observability, large fault-induced transients, reduction in the stability margin, even loss of the closed-loop system stability.

The design of FTCS not only involves a wide range of subject areas, such as dynamic system modelling, modern control theory, advanced signal processing, and real-time statistical decision-making, but also deals with interactions of these subjects in a real-time environment. The real-time nature of the problem can never be underestimated.

1.2 Development of Fault Tolerant Control Systems Design Techniques

As mentioned earlier, the most important consideration in FTCS is how to maintain system stability and the acceptable performance in the presence of component failures. Early efforts in the development of FTCS were mainly focused on passive fault tolerant approaches. The design issues associated with inherent redundancy in multivariable systems were examined in the context of passive FTCS design. An important concept known as the system integrity, was introduced by MacFarlane, [2]. The multivariable system possessing integrity implies that the entire closed-loop system remains stable in the event of component failures in some loops. Such a concept has been adopted as a very important design objective in the development of passive fault tolerant control systems. Necessary and sufficient conditions for the multivariable system possessing integrity against actuator failures and sensor/actuator failures have been derived in [3], [4] and [5], respectively.

There are several control system design techniques that can be tailored to the design of passive FTCS. Some researchers have applied optimal control techniques to the design of the control systems possessing integrity. A design approach for passive FTCS against actuator failures was developed by solving a Riccati-type equation and using a state feedback control, [6]. A similar problem was also solved by means of a matrix Lyapunov equation in [7]. It should be noted that the methods are only applicable to open-loop asymptotically stable systems. By restricting the modes of actuator failures to a specific set, two types of design approaches based on linear quadratic control were proposed in [8] and [9], where both stable and unstable open-loop systems can be dealt with. Several important design issues related to the centralized and decentralized fault tolerant control

systems with guaranteed stability have been discussed in [10] for sensor and actuator failures in a pre-specified set. The advantage of this approach is that the performance of the control system in the event of component failures can be measured in terms of an H_∞ norm bound. This design approach has further been extended to discrete systems using δ -operator methodology in [11].

Another type of design technique which has been applied to the passive FTCS design is the parametric space method for robust control [12]. Also related is a graphic-oriented design scheme proposed in [13]. With a proper choice of controller structure and the combination of its parameters, the closed-loop control system can be made insensitive to sensor and actuator failures.

In the late seventies, a multiple disjoint decentralized control structure was studied analytically in [14]. Redundancy in such a control system structure is introduced as multiple controllers. Decentralized state feedback control strategies were used to synthesize these multiple controllers. It was shown that the synthesis problem can be reduced to the problem of simultaneous stabilization, in which a single control law is synthesized to stabilize multiple systems [15]. In the context of FTCS, a single system with different component failures can be described by multiple system representations. By using such a structure and design method, reliability of the overall system can be improved beyond that of the individual controller [14]. The dual problem of simultaneous stabilization is known as reliable stabilization, in which a set of controllers are designed to stabilize a single system [16]. Any controller in the set or any combination of them will be able to stabilize the system. Obviously, fault tolerance is achieved by such a control strategy.

With a better understanding of the roles that redundant actuators play in a dynamic system, a new approach to the design of FTCS against actuator failure was developed [17]. The uniqueness of this approach is the introduction of a dynamic pre-compensator which makes the dynamic relationships from each actuator channel to the system output similar (they can differ by scale factors), so that the form of system redundancy are

simplified. The advantage of this approach is that the physical insight in the design is clear, and the design procedure is straightforward. This scheme can be used to stabilize open-loop unstable systems, provided that there is at least one healthy actuator. By incorporating a *PI* (Proportional and Integral) control scheme, this design approach can maintain not only the closed-loop stability, but also the steady-state tracking ability in the presence of actuator failures [18].

As for passive FTCS, the failure modes are among the anticipated ones. To deal with unanticipated failures, active FTCS are more appropriate. Research activities in active FTCS mainly focus on the following two areas: (i) real-time fault detection and identification (FDI), and (ii) real-time control system reconfiguration. Within each area, a significant amount of work has been done. However, we have to realize that one of the key problems in active FTCS is how to combine these two parts in a real-time environment. It is important that the research and development in both areas not be carried out entirely independently.

A tremendous amount of work has been done in the area of FDI in the last two decades. Many techniques have been developed. The existing methods can be classified into two categories: (i) model-free; and (ii) model-based, FDI schemes. Since the design of a reconfigurable controller relies heavily on the post-fault information on the system, model-based FDI techniques are more appropriate for active FTCS. Essentially, a model-based FDI scheme utilizes knowledge of the system model to carry out FDI in real-time. The three most commonly used techniques are based on: (i) state estimation; (ii) parameter estimation; and (iii) the parity equation. Several excellent survey papers are available on these subjects [19][20][21][22][23]. The relationship among these approaches has been investigated recently in the context of FTCS in [24]. It was found that state estimation based schemes are better suited for fault detection since they are inherently fast and cause short time delays in the real-time decision-making process. However, the information from state estimation based algorithms alone may not be detailed enough for the subsequent control system reconfiguration. Parameter estimation based schemes are more suit-

able in this respect, since they can provide information on post-fault system parameters. Hence, by using the state estimation scheme for fault detection and the parameter estimation scheme for fault identification, one can detect faults quickly and obtain detailed fault information at the same time. This will definitely benefit the subsequent control reconfiguration process.

The reported work of active FTCS traces back to 1985 when an automatic redesign approach was developed against control element failures for commercial aircraft, [25]. The design procedure was based on a linear quadratic methodology which redistributed the control authority of the failed control surfaces to the remaining surfaces. From the view point of performance recovery following a failure, a pseudo-inverse based control system reconfiguration method was extensively examined in [26]. A necessary modification to the original scheme was made such that the stability of the closed-loop system after reconfiguration is maintained. One of the advantages of the pseudo-inverse method for reconfigurable control design is the simplicity of calculating the feedback controller gain matrix. By embedding the desired system performance into a reference model, a novel reconfigurable control system design scheme using a perfect model following principle has been proposed in [27]. It was shown therein that there exists a close tie between the perfect model following and the pseudo-inverse approaches. In order to effectively recover the performance of the original system, an eigenstructure assignment based algorithm was proposed in [28] for both state and output feedback cases. In this approach, eigenvalues and eigenvectors of the post-fault system can be assigned in an optimal way so that the maximal performance recovery can be achieved.

Most of the research work in the field of reconfigurable control has been carried out with the assumption that a perfect post-fault system model is available, under which the objective of reconfigurable control is only to stabilize the post-fault system and to recover the original system performance. However, to design an effective active FTCS, the FDI and reconfigurable control schemes should be integrated in the design process and work in harmony in a real-time environment. In [29], an approach using a four parameter

controller was proposed to integrate the fault detection and the control reconfiguration, with special considerations on the interaction between the FDI module and reconfigurable control module. Recognizing the fact that a well designed robust control system may hinder the sensitivity of FDI schemes, an H_∞ based performance specification is proposed in [30], where a parametrized set of controllers satisfying a prescribed performance level is constructed first, and then the parameter is optimized to maximize the sensitivity for the purpose of fault detection.

Since system component failures often result in a reduction in the stability margin of the system, it is highly desirable that the fault in the system be detected promptly to maintain the integrity of the entire system, and the corrective control actions are taken swiftly. With a clear understanding of this problem, a completely new design methodology for active FTCS has been developed in [31]. The scheme utilizes a bounding parameter estimation algorithm with a parametric robust control design technique. Once the occurrence of a fault is detected, the bounding parameter estimation scheme is used to obtain the bounds on the post-fault system parameters. A robust controller can immediately be synthesized based on the established bounds to start stabilizing the system. As more data becomes available, the bounds become tighter, the control system performance will be gradually improved and recovered as much as possible.

For any practical system, the fault occurrence time is usually random. The system disturbances and the measurement noise are random in nature as well. With all these sources of randomness, it is not too difficult to imagine that the characteristics of active FTCS can also be random, therefore can be more adequately described from a stochastic point of view. With the assumption that the mechanism of actuator failures can be captured by a Markov chain, an optimal control strategy has been developed using dynamic programming approach of Birdwell *et al.* Once a failure has occurred in the system, the pre-calculated feedback gain matrices are switched accordingly to maintain the closed-loop system stability in a stochastic sense, [32]. With a set of pre-assumed failure modes, the dynamic system can often be characterized by a set of dynamic models. Based on such a

multiple model representation, Maybeck *etal.* have developed adaptive control algorithms to deal with anticipated component failures [33]. The theoretical aspects of such multiple model adaptive control have been further examined in [34]. With appropriate assumptions on the stochastic behaviors of all random sources in active FTCS, stochastic stability of active FTCS can be analyzed. It was shown that excessive time delay in the FDI scheme will contribute adversely to the stability of the closed-loop system [35]. This approach has further been extended to the situation where two stochastic processes were used to represent, respectively, failures of system components and the behavior of FDI decisions in [36].

Since active FTCS involve real-time FDI and controller reconfiguration, it appears to possess certain degree of intelligence. Therefore, such types of systems have also been classified as *intelligent* control systems. Intelligent control, in general, also covers other approaches such as fuzzy logic and neural network based control schemes [37]. But nevertheless, active FTCS is an important part of intelligent control systems. Various aspects of active FTCS have been discussed in the framework of the intelligent control systems in [38] [39] [40].

Along with the increasing automation level and reliability requirement of control systems and processes, FTCS design methodology has been utilized in various applications, including aircraft [41] [42], space shuttle [43], autonomous underwater vehicles [44], nuclear reactors [45][46], and power systems [47].

1.3 Scope of the Thesis

Although research on FTCS can be conducted in both deterministic and stochastic domains, in this thesis the design and analysis of FTCS is mainly in the deterministic domain. It also should be pointed out that faults in practical systems may result in certain nonlinearities, which may be more appropriate to handle using nonlinear control theory. However, throughout this thesis, we will only consider linear systems (or the linear

operation range of the system). The thesis has seven chapters. The general concepts as well as special design considerations associated with FTCS are described in Chapters 2 and 3. These two chapters establish the foundation for further investigation of FTCS. Chapter 4 is devoted to the synthesis of passive FTCS against actuator and sensor failures. The design of active FTCS is the subjects of Chapters 5 and 6. The design considerations of real-time fault detection and identification schemes are addressed in Chapter 5 and the design of the control reconfiguration scheme is illustrated in Chapter 6. Finally, Chapter 7 concludes the thesis and summarizes the future work.

1.4 Bibliography

- [1] B. W. Johnson, *Design and Analysis of Fault Tolerant Digital Systems*, Addison-Wesley Publishing Company, Inc., New York, 1989.
- [2] A. G. J. MacFarlane, *Complex Variable Methods for Linear Multivariable Feedback Systems*, Taylor and Francis Ltd., London, 1980.
- [3] M. Fujita and E. Shimemura, "Integrity against arbitrary feedback-loop failure in linear multivariable control systems," *Automatica*, vol. 24, no. 6, pp. 765-772, 1988.
- [4] V. R. Sule, "Design of feedback controllers with integrity," *Control Theory and Advanced Technology*, vol. 7, no. 2, pp. 285 - 299, 1991.
- [5] A. N. Gundes, "Stability of feedback systems with sensors or actuators failures: analysis," *International Journal of Control*, vol. 56, no. 4, pp. 735-753, 1992
- [6] E. Shimemura and M. Fujita, "A design method for linear state feedback systems possessing integrity based on a solution of a Riccati-type equation," *International Journal of Control*, vol. 42, no. 4, pp. 887-899, 1985.

- [7] L. S. Shieh, H. M. Dib, S. Ganesan and R. E. Yates, "Optimal pole-placement for state-feedback systems possessing integrity," *International Journal of Systems Science*, vol. 19, no. 8, pp. 1419-1435, 1988.
- [8] S. M. Joshi, "Design of failure-accommodation multiloop LQG-type controllers," *IEEE Trans. on Automatic Control*, vol. 32, no. 8, pp. 740-741, 1987.
- [9] R. J. Veillette, "Reliable linear - quadratic state-feedback control," *Automatica*, vol. 31, no. 1, pp. 137-143, 1995.
- [10] R. J. Veillette, J. V. Medanic and W. R. Perkins, "Design of reliable control systems," *IEEE Trans. on Automatic Control*, vol. 37, no. 3, pp. 290 -304, 1992.
- [11] M. H. Shor, W. R. Perkins and J. V. Medanic, "Design of reliable decentralized controllers: a unified continuous/discrete formulation," *International Journal of Control*, vol. 56, no. 4, pp. 943 - 965, 1992.
- [12] D. D. Siljak, "Parameter space methods for robust control design: a guided tour," *IEEE Trans. on Automatic Control*, vol. 34, no. 7, pp. 674 - 688, 1989.
- [13] J. E. Ackermann, *Robust Control: Systems with Uncertain Physical Parameters*, Springer-Verlag, New York, 1993.
- [14] D. D. Siljak, "Reliable control using multiple control systems," *International Journal of Control*, vol. 31, no. 2, pp. 303-329, 1980.
- [15] M. Vidyasagar, *Control Systems Synthesis: A Factorization Approach*, North Holland System and Control Series (Vol. 8), MIT Press, Cambridge, M.A, 1985.
- [16] M. Vidyasagar and N. Viswanadham, "Algebraic design techniques for reliable stabilization," *IEEE Trans. on Automatic Control*, vol. AC- 27, pp. 1085 - 1095, 1982.

- [17] Q. Zhao and J. Jiang, "Reliable state feedback control system design against actuator failures," *Automatica*, vol. 34, no. 10, pp. 1267-1272, 1998.
- [18] J. Jiang and Q. Zhao, "Design of reliable control systems possessing actuator redundancies," submitted to *AIAA (American Institute of Aeronautics and Astronautics) Journal of Guidance, Control and Dynamics* in March, 1999.
- [19] A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, no. 6, pp. 601-611, 1976.
- [20] R. Isermann, "Process fault detection based modelling and estimation methods: A survey," *Automatica*, vol. 20, no. 4, pp. 387-404, 1984.
- [21] J. Gertler, "Survey of model-based failure detection and isolation in complex plants," *IEEE Control Systems Magazine*, vol. 8, no. 6, pp. 3-11, 1988.
- [22] R. Patton, P. Frank and R. Clark, *Fault Diagnosis in Dynamic Systems, Theory and Application*, edited, Prentice Hall Ltd., UK, 1989.
- [23] P. M. Frank, "Fault diagnosis in dynamic system using analytical and knowledge based redundancy - a survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459-474, 1990.
- [24] J. Jiang and Q. Zhao, "Comparison of RLS parameter and state estimation based FDI schemes," submitted to *Journal of Franklin Institute* in January, 1999.
- [25] D. P. Looze, J. L. Weiss, J. S. Eterno and N. M. Barrett, "An automatic redesign approach for restructurable control systems," *IEEE Control Systems Magazine*, pp. 16-22, May, 1985.
- [26] Z. Gao and P. J. Antsaklis, "Stability of the pseudo-inverse method for reconfigurable control systems," *International Journal of Control*, vol.53, no.3, pp. 717-729, 1991.

- [27] Z. Gao and P. J. Antsaklis, "Reconfigurable control system design via perfect model following," *International Journal of Control*, vol. 56, no. 4, pp. 783-798, 1992.
- [28] J. Jiang, "Design of reconfigurable control systems using eigenstructure assignment," *International Journal of Control*, vol. 59, no. 2, pp. 395-410, 1994.
- [29] C. A. Jacobson and C. N. Nett, "An integrated approach to controls and diagnostics using the four parameter controller," *IEEE Control Systems Magazine*, pp. 22-29, October, 1991.
- [30] N. E. Wu and T. J. Chen, "Feedback design in control reconfigurable system," *International Journal of Robust and Nonlinear Control*, vol. 6, pp. 561 - 570, 1996.
- [31] J. Jiang and Q. Zhao, "Reconfigurable control based on imprecise fault identification," *Proc. of 1999 American Control Conference*, San Diego, U.S.A, pp. 114-118, June, 1999.
- [32] J. D. Birdwell, D. A. Castanon and M. Athans, "On reliable control system designs," *IEEE Trans. on Systems, Man and Cybernetics*, vol. SMC-16, no. 5, pp. 703-711, 1986.
- [33] P. S. Maybeck and R. D. Stevens, "Reconfigurable flight control via multiple model adaptive control methods," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 27, no. 3, pp. 470-480, 1991.
- [34] K. S. Narendra and J. Balakrishnan, "Adaptive control using multiple models," *IEEE Trans. on Automatic Control*, vol. 42, pp. 171-187, 1997.
- [35] M. Mariton, "Detection delays, false alarm rates and the reconfiguration of control systems," *International Journal of Control*, vol. 49, no. 3, pp. 981-992, 1989.

- [36] Srichander, R. and B. K. Walker, "Stochastic stability analysis for continuous time fault-tolerant control systems," *International Journal of Control*, vol. 57, no. 2, pp. 433-452, 1993.
- [37] R. F. Stengel, "Toward intelligent flight control," *IEEE Trans. on Systems, Man & Cybernetics*, vol. 23, no. 6, pp. 1699-1717, 1993.
- [38] R. F. Stengel, "Intelligent failure-tolerant control," *IEEE Control Systems Magazine*, vol. 11, no. 4, pp. 14-23, 1991.
- [39] H. E. Rauch, "Intelligent fault diagnosis and control reconfiguration," *IEEE Control Systems Magazine*, pp. 6 - 12, June, 1994.
- [40] H. E. Rauch, "Autonomous control reconfiguration," *IEEE Control Systems Magazine*, pp. 37-48, December, 1995.
- [41] S. D. Zemlyakov, V. Y. Rutkovskii and A. V. Silaev, "Reconfiguring aircraft control systems in case of failures," *Automation and Remote Control*, vol. 57, no. 1. pp. 1-13, 1996.
- [42] P. R. Chandler, M. Pachter and M. Mears, "System identification for adaptive and reconfigurable control," *AIAA Journal of Guidance, Control and Dynamics*, vol. 18, no. 3, pp. 516 - 524, 1995.
- [43] H. V. Panossian and W. D. Ewing, "Real-time failure detection algorithm for the space shuttle main engine," *IEEE Control Systems Magazine*, vol. 17, no. 4, pp.16 - 23, 1997.
- [44] J. Farrell, B. D. Appleby, and T. Berger, "On the detection and accommodation of unanticipated faults," *Proc. of 1992 AIAA Guidance, Navigation and Control Conf.*, Hilton Head Island, SC, pp. 1045-1054. AIAA-92-4537-CP, 1992.

- [45] H. E. Garcia, A. Ray and R. M. Edwards, "Reconfigurable control of power plants using learning automata," *IEEE Control Systems Magazine*, pp. 85-92, January, 1991.
- [46] E. Eryurek, and B. R. Upadhyaya, "Fault-tolerant control and diagnostics for large-scale systems," *IEEE Control Systems Magazine*, pp. 34-42, October, 1995.
- [47] S. A. Merryman and R. M. Nelms, "Diagnostic technique for power systems utilizing infrared thermal imaging," *IEEE Trans. on Industrial Electronics*, vol. 42, no. 6, pp. 615 - 628, December, 1995.

Special Considerations in Fault Tolerant Control Systems

2.1 Introduction

As illustrated in Chapter 1, the objective of FTCS is to compensate for system component failures/faults so that the desired system performance can be maintained. In comparison with conventional control systems, there exist many special considerations in FTCS, such as system modelling, design objectives, performance degradation and its measure. In this Chapter, these special considerations will be illustrated in detail. First, characteristics of different system component failure/faults are analyzed, and different fault scenarios are mathematically modelled in a unified framework. Secondly, design objectives of FTCS are discussed followed by the performance specifications of FTCS in different operational stages.

2.2 Characteristics of Dynamic Systems with Faults

2.2.1 Faults in dynamic systems

Elements in a control system include sensors, actuators, controllers, and the plant being controlled. The system usually works in a closed-loop configuration. Any abnormal operations among these components are referred to as faults. Faults can occur in various degrees of severity and at random times. Generally speaking, faults can be classified either according to their physical locations in the system, or their effects on the system performance. Fault classifications based on physical locations have been adopted in this thesis because such classifications allow us to associate faults with system redundancy

directly. Depicted in Figure 2.1 are the faults that could occur in different elements of the system.

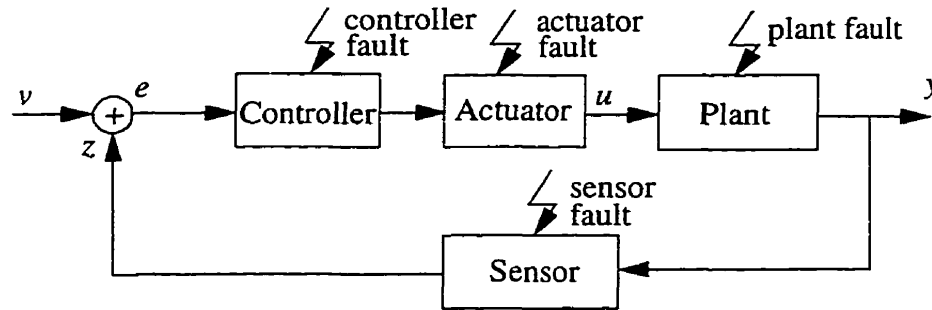


Figure 2.1 Component faults in a closed-loop control system

Sensor faults are incorrect readings due to malfunctions in sensory elements or transducers, such as broken wires, loss of effectiveness, unknown bias at the sensor output as a result of poor calibration, or even unexpected changes in the dynamic characteristics of the transducers. Since the signal from a sensor often carries the most important information in a feedback control system, the state of the health of the sensor is therefore crucial for the reliable operation of the entire system.

Faults in actuators can range from the control element being stuck at a fixed value and changes in the control element's dynamic characteristics, to a total loss of the control capabilities. When an actuator fault occurs, any change in the actuator input will no longer produce any desired response at the actuator output. In other words, the control signal will not pass through this actuator channel correctly. The wrong control action will undoubtedly jeopardize the performance of the entire system.

Since most modern controllers are in software form, faults in controllers are often associated with software bugs. On the hardware side, we usually classify faults in A/

D and D/A converters as sensor and actuator faults, respectively. We will in general describe dynamic system faults in the plant as large abrupt changes in system parameters.

By and large, faults can occur in many different ways in a control system, and it is not straightforward to obtain the cause-effect relationship for every fault. Hence, it is usually difficult to perform the design and analysis of FTCS, even at the modelling stage. The mathematical representation of the system with faults needs to be carefully examined. In the next section, various types of faults in a control system will be described, and modelled.

It should be noted that the faults considered in this thesis are those which can be handled by properly designed FTCS. In other words, we will not consider non-recoverable faults, which lead to the complete loss of the system controllability/observability, such as disintegration of an airplane, or total failure of a power source.

2.2.2 Modelling of faults

Consider a system in an open-loop form, containing actuators, sensors, controllers, and the plant, its block diagram is illustrated in Figure 2.2, where the dynamic characteristics of these components are shown in terms of transfer functions. As mentioned earlier, faults can occur in all these components.

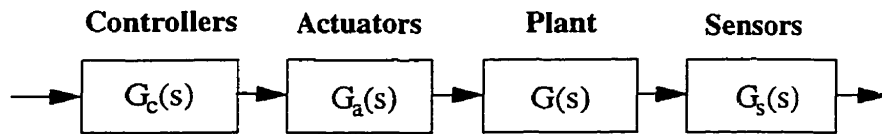


Figure 2.2 Elements in a control system

For the sake of simplicity and to avoid any confusion, in the subsequent analysis, the dynamics associated with sensors, actuators, and controllers is assumed to be

lumped together with the plant dynamics. Therefore, faults associated with the dynamics in these system elements can often be treated as plant dynamic faults in the mathematical model.

1. Fault-free system model

- State-space model

The fault-free plant can be represented in the following state-space form:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t)\end{aligned}\tag{2.1}$$

where $x \in \mathbb{R}^{n \times 1}$, $u \in \mathbb{R}^{m \times 1}$, and $y \in \mathbb{R}^{p \times 1}$ are the system state, input and output vectors, respectively. The matrices, $A \in \mathbb{R}^{n \times n}$ is the system matrix, $B \in \mathbb{R}^{n \times m}$ and $C \in \mathbb{R}^{p \times n}$ are the input and output matrices, respectively. They can further be written into the following forms:

$$B = \begin{bmatrix} B_1 & B_2 & \dots & B_m \end{bmatrix}\tag{2.2}$$

$$C = \begin{bmatrix} C_1 & C_2 & \dots & C_p \end{bmatrix}^T\tag{2.3}$$

where B_i , $i = 1, 2, \dots, m$ are $n \times 1$ column vectors, and C_j , $j = 1, 2, \dots, p$, are $1 \times n$ row vectors.

Based on the system representation in EQ (2.1), system elements can also be depicted in Figure 2.3.

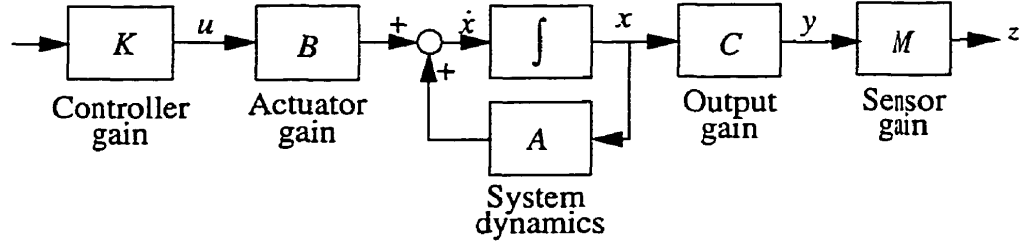


Figure 2.3 System elements in the state-space representation

Compared with Figure 2.2 with the physical meaning of the above block diagram in mind, it is important to point out that the matrix A includes not only the dynamics of the plant, but also those of the sensors, the actuators, and the controllers. It should be emphasized that the matrix C does not represent system sensors in any way. Sensors can be viewed as dynamic elements (devices) that expose (measure) system outputs. Therefore, the relationship between system outputs and sensor outputs can best be described by:

$$z(t) = My(t) \quad (2.4)$$

or

$$z(t) = MCx(t) = \tilde{M}x(t) \quad (2.5)$$

where $z \in \mathbb{R}^{q \times 1}$ represents the sensor outputs. $M \in \mathbb{R}^{q \times p}$ and $\tilde{M} \in \mathbb{R}^{q \times n}$ can be called sensor gain matrices. M relates the measured system outputs to the sensor outputs, while $\tilde{M}$ relates the measured system states to the sensor outputs. It is proposed that sensor faults should be modelled in M or $\tilde{M}$, instead of C .

It should be noted that in the existence of multiple sensor redundancy, the number of the sensor outputs is greater than the number of the system outputs/states. In other words, the dimension of the sensor output vector, z , is greater than that of the system output/state vector, y or x , i.e. $q > p$ in M and $q > n$ in $\tilde{M}$. When there is no sensor redun-

dancy, the dimension of sensor output vector should be equal to that of the output/state vector, i.e. $q = p$ in M and $q = n$ in $\tilde{M}$. The concept of sensor redundancy will be further detailed in Chapter 3.

It should be pointed out that although the above state-space representation in EQ (2.1) is for continuous time systems, a similar form applies to the discrete-time case as well.

- Transfer function

Based on the system state-space representation, the system transfer function can then be obtained:

$$Y(s) = G(s) U(s)$$

$$G(s) = C(Is - A)^{-1}B = \{C_i(Is - A)^{-1}B_j, i = 1, 2, \dots, p, j = 1, 2, \dots, m\} \quad (2.6)$$

- ARMA model

Given a LTI (Linear Time-Invariant) discrete-time SISO (Single Input and Single Output) system, it can also be modelled using an ARMA model.

$$y(k) + a_1 y(k-1) + a_2 y(k-2) + \dots + a_n y(k-n) = b_1 u(k-1) + \dots + b_r u(k-r) \quad (2.7)$$

or as:

$$y(k) = \psi^T(k) \theta_o \quad (2.8)$$

$$\psi^T(k) = [-y(k-1), -y(k-2), \dots, -y(k-n), u(k-1), \dots, u(k-r)] \in \mathbb{R}^{(n+r) \times 1} \quad (2.9)$$

where $\psi(k)$ is the regression vector, $u(k)$ and $y(k)$ are the sampled system input and output, respectively. $\theta_o = [a_1 \dots a_n b_1 \dots b_r]^T \in \mathbb{R}^{(n+r) \times 1}$ represents nominal system parameters.

2. System dynamic faults

As illustrated earlier, the system dynamics include the dynamics of all system components, such as sensors, actuators, controllers, and the plants. Faults in these components that cause changes in the dynamic relationship of the system, are referred to as system faults. In most situations, such faults will change physical parameters of the system, e.g. resistance, the gain of an amplifier, etc. These changes will manifest themselves as parameter changes in the mathematical model describing the system.

To be more precise, a fault in system dynamics can be expressed as:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) & t < t_f \\ \dot{x}(t) = (A + \Delta A)x(t) + (B + \Delta B)u(t) & t \geq t_f \end{cases} \quad (2.10)$$

and

$$\begin{cases} y(t) = Cx(t) & t < t_f \\ y(t) = (C + \Delta C)x(t) & t \geq t_f \end{cases} \quad (2.11)$$

where t_f is the time instance at which the fault has occurred, and ΔA contains fault-induced changes in the system dynamics. ΔB and ΔC reflect the fault induced changes in the input matrix and the output matrix, respectively. Generally speaking, the size of ΔA , ΔB and ΔC depends on the severity of the fault. They are usually unknown *a priori* for active FTCS.

In the case of the ARMA model, system faults are modelled as jumps in coefficients in the equation. Such a representation has been employed in Chapter 5 for both FDI and controller reconfiguration.

$$\begin{cases} y(k) = \psi^T(k) \theta_o & k < k_f \\ y(k) = \psi^T(k) (\theta_o + \Delta\theta) & k \geq k_f \end{cases} \quad (2.12)$$

where k_f is the time of the fault occurrence, and $\Delta\theta$ contains the fault induced parameter changes.

3. Actuator failures/faults

As mentioned earlier, an actuator is a device that manipulates the control variable, and delivers the control action to the physical system. Failures in actuators can have severe consequences on the performance of the system. No matter how good the controller is, the control signal cannot get through to the system without a healthy actuator.

Since faults that cause changes in the actuator dynamics are modelled as system dynamic faults, which have been discussed in the preceding section, by actuator fault we mean any other non-dynamic related faults in the actuator, such as loss in the gain, and the control elements being stuck at certain value. Without loss of generality, such fault scenarios can be modelled by relating the actuator output signal, $u_a(t)$, to its input signal, $u(t)$, as:

$$u_a(t) = L_a u(t) + (I_m - L_a) \cdot f_a \quad (2.13)$$

where the matrix $L_a \in \mathbb{R}^{m \times m}$ has the following structure:

$$L_a = \begin{bmatrix} l_1 & 0 & 0 & 0 \\ 0 & l_2 & 0 & 0 \\ 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & l_m \end{bmatrix} \quad (2.14)$$

where I_m is an $m \times m$ identify matrix, and $f_a \in \mathbb{R}^{m \times 1}$ contains the values at which the actuators are stuck. The i th diagonal element l_i is a binary indicator, which corresponds to the health state of the i th control channel,

$$l_i = \begin{cases} 1 & t < t_f \\ 0 & t \geq t_f \end{cases} \quad (2.15)$$

The above failure model is only suitable for complete actuator outage. The situation where the actuator undergoes a partial failure can generally be modelled by changes in the input matrix, i.e. ΔB .

4. Sensor failures/faults

A sensor is a device that is not only for measuring the system output for the purpose of feedback control, but also for exposing some of internal system variables for the purpose of performance monitoring. From a feedback control point of view, the accuracy of the information provided by the sensor will ultimately determine the performance of the control system. Even a minor fault in the feedback sensor can have a severe consequence, because the controller may take the wrong action based on the wrong information.

In practice, in addition to the dynamic changes in the transducer, there are two other common types of sensor failures: (i) gain reduction; and (ii) constant unknown bias. These situations can be modelled as:

$$y_s = L_s M y + (I_s - L_s) \cdot f_s \quad (2.16)$$

where the matrix $L_s \in \mathbb{R}^{q \times q}$ is similarly defined to EQ (2.14) and EQ (2.15), $I_s \in \mathbb{R}^{q \times q}$ is an identity matrix, and $f_s \in \mathbb{R}^{q \times 1}$ corresponds to the unknown bias term.

It is important to point out that, unlike actuators, redundant sensors are usually much easier to install in a system. Therefore, the strategies for FTCS design against sensor faults may differ from those against actuator faults. One approach to deal with sensor faults is to employ multiple dissimilar sensors to measure the same system variable. The sensor outputs are then compared, and the most reliable readings are selected using a vot-

ing scheme, [1]. To obtain a consistent measurement, at least three sensors should be used. Another effective method is to install redundant sensors at different measurement points. These sensors can produce measurements on other intermediate system variables. Using the mathematical models between the desired system outputs and these intermediate system variables, additional information on the system outputs can be calculated. This type of scheme is referred to as hybrid redundant sensors, which will be discussed in Chapter 3. In industry, it is also common to use sensors with self-diagnosis capabilities that can flag any abnormalities should they occur. This type of sensors are often known as intelligent sensors.

5. Additive and multiplicative faults

In the above discussions, faults/failures are classified and modelled, according to their physical locations, into system faults, actuator fault and sensor faults. It needs to be pointed out that these faults can also be modelled according to their effects on the system outputs and the system dynamics. In this case, they are classified into additive and multiplicative faults, [2]. In order to be consistent with the modelling of the faults described in the previous sections, in this section, the additive and multiplicative faults are also modelled in two different system representation forms: state-space representation and ARMA model.

A. Additive faults

Definition 2.1 (Additive faults, [2])

By taking into account random noise in the system, any faults in the system components that result in changes only in the mean value of the system output signal (observation sequences) are called additive faults.

- State-space model

Consider the system described by the state-space representation in EQ (2.1), the additive fault can be modelled in the following forms:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + \Delta_u \\ y(t) &= Cx(t) + \Delta_y \end{aligned} \quad t \geq t_f \quad (2.17)$$

where $\Delta_u \in \mathbb{R}^{n \times 1}$ and $\Delta_y \in \mathbb{R}^{p \times 1}$ are vectors that contain the fault induced changes in state transition equation and in output observation equation, respectively. It should be pointed out that the above fault only results in changes in the mean of the output observation, $y(t)$.

- ARMA model

The additive faults can also be represented in the ARMA model of the system:

$$y(k) = -\sum_{i=1}^n a_i y(k-i) + \sum_{j=1}^q b_j [u(k-j) + \delta_u(k-j)] \quad k \geq k_f \quad (2.18)$$

where $\delta_u(k-j)$, $j = 1, 2, \dots, q$ is the additive fault occurring at k_f .

Usually, additive faults do not change the system dynamics. It is clear that when the control element of an actuator is stuck at a fixed value, the output of the actuator appears to be an unknown constant input (disturbance) to the system. This type of actuator fault belongs to the additive faults. Similarly, the sensor fault that causes a sensor bias is also an additive fault. As it will be shown in Chapter 5, such type of faults is relatively easy to detect.

B. Multiplicative faults

Definition 2.2 (Multiplicative faults, [2])

By taking into account random noise in the system, any faults in the system components that result in changes in the variance, correlations of the system output signal as well as changes in the spectral characteristics and dynamics of the system are called multiplicative faults.

- State-space model

Consider the system described in EQ (2.1), the multiplicative fault can be modelled in the following form:

$$\dot{x}(t) = (A + \Delta A)x(t) + (B + \Delta B)u(t) \quad t \geq t_f \quad (2.19)$$

The above modelled fault results in the changes in the system dynamics. More precisely, the fault induced change in B matrix will result in changes in the variance of the output observation, while that in A matrix will result in changes in the system spectrum.

- ARMA model

The multiplicative faults can also be modelled in ARMA model.

$$y(k) = -\sum_{i=1}^n (a_i + \Delta a_i) y(k-i) + \sum_{j=1}^q (b_j + \Delta b_j) u(k-j) \quad k \geq k_f \quad (2.20)$$

From the above models, it can be seen that the system faults are multiplicative faults in nature. They can have serious consequences on the overall system behavior, such as abnormal changes in system dynamic characteristics and even instability. For actuator faults and sensor faults, from EQ (2.13) and EQ (2.16), they can be additive or multiplicative.

6. Fault-induced Transients in Dynamic Systems

From the above analysis, it is clear that faults can often result in large and sudden changes in the system dynamics, sensors, or actuators. Inevitably, these changes will introduce transients in the corresponding system variables. These fault-induced transients are potentially harmful to the overall operation of the system.

When a fault occurs, there are three major sources of transients which warrant some special consideration. The first one is due to the sudden breakdown of system com-

ponents that may create some imbalance among otherwise balanced system variables. These types of transients may not have a fixed pattern, and their impact on the system is highly dependent on the operating conditions of the system at the time of the fault.

The second type of transients relate directly to the natural modes of the system. In a closed-loop system, if the impairment of system sensors/actuators prevents the control signals from reaching the system effectively, the system may, in fact, operate momentarily in an open-loop fashion. Any poorly damped open-loop modes will result in transients and the amplitude of this type of transients may grow with time. If no appropriate control actions are taken promptly, these transients may eventually drive the system into a non-recoverable state. To reduce these types of transients, the control system has to react quickly and precisely to the fault. These types of transients, if dealt with inadequately, can jeopardize the stability of the entire system.

The third class of transients are pertinent only to active FTCS. In an active FTCS, the parameters and/or structures of the controller have to be adjusted in real-time in response to the system failures. Due to the complexity of the control schemes, it may be difficult to perfectly match the values of the related system variables before and after the adjustment. Such mis-match can lead to short periods of transients in the system variables.

A typical pattern of a transient in a system variable, $x_i(t)$, is illustrated in Figure 2.4. We often characterize a transient by its total power and the peak amplitude. In Figure 2.4, the peak amplitude of the transient is shown as x_{max} , and the total power can be conveniently measured by:

$$P = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} [x_i(\tau) - x_{s,i}]^2 d\tau \quad (2.21)$$

where $x_{s,i}$ is the steady-state value of $x_i(t)$.

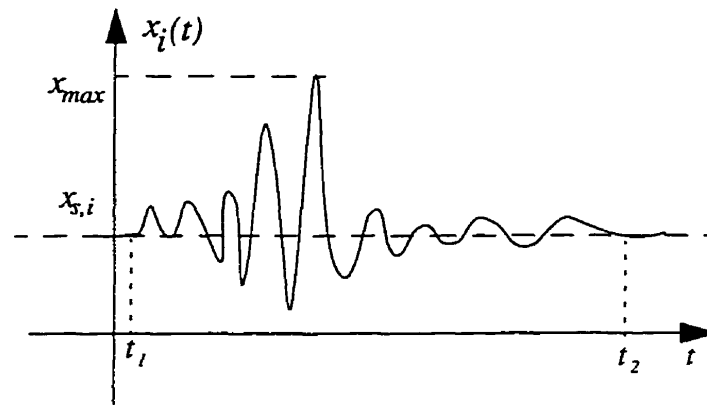


Figure 2.4 Transients in a dynamic system

The peak amplitude and the total power of the transients reflect the severity of faults as well as the ability of the control system in dealing with them. In fact, it will be shown later that one of the design objectives in active FTCS is to suppress the development of these fault-induced transients shortly after the occurrence of faults.

2.3 Design Objectives of FTCS

To design a control system, there are always three main issues that one should consider carefully. The first is to decide what are the most important objectives that the control system is intended to achieve; the second is to decide what are the most effective measures to evaluate these objectives. Finally, how can one synthesize an appropriate controller to achieve these objectives.

The uniqueness of FTCS is that the design objectives should contain not only the specifications for normal system operation, but also for the system under fault conditions. When specifying the system performance, one should balance the design objectives in both situations. It is important to point out that the emphasis on the system performance can be completely different in these two modes of operation. During the normal operation, more concern should be placed on the quality of the system behavior. While in the pres-

ence of faults, the robustness of the system, and how the system survives with an acceptable performance degradation, become the more important issues.

To be more precise, one can assign priorities among the design objectives and rank them according to their importance and the potential influence on system behaviors. This priority list should cover the system operating status under all conceivable conditions. Generally speaking, this list can be divided into two groups: primary (high-priority) objectives, and secondary (low-priority) objectives. The primary objectives correspond to the most critical system properties. Violation of these objectives will certainly have some serious consequences. A good example is the aircraft flight control. Here, the primary objective of a flight control system is to maintain the stability and the safety of the aircraft at all time. Secondary objectives may include things like fuel efficiency, maneuverability, and the optimal flight speed. Under normal flight conditions, efforts should be made to achieve not only the primary, but also the secondary objectives. However, in the event of an emergency, the most important objective is to maintain the stability of the aircraft and to land the aircraft safely, and the secondary objectives become far less important.

In this context, a fault tolerant control system should be designed such that the high priority objectives are achieved first. When a fault occurs, depending on the nature and the severity of the fault, the system should be able to give up some secondary design objectives so that the primary objectives can be maintained with minimal performance degradation. This concept can be illustrated in Figure 2.5 where the left column represents the objective list for the system under normal operation. When a fault has occurred, the FTCS should attempt to achieve the high priority objectives first with some sacrifice in the low priority ones.

The ability of the control system, in the event of a fault, to automatically reduce its demand on the level of performance so that the high priority objectives are maintained first is known as the *graceful degradation*. This is an important quality of FTCS that makes FTCS unique.

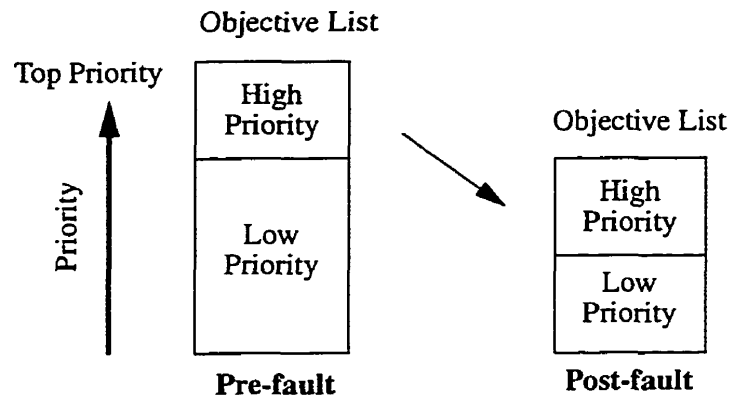


Figure 2.5 Objective list of FTCS

To achieve the fault tolerance, there must be some redundancies in the system. In fact, what makes FTCS different from other conventional control systems is the existence of these redundancies, and the ability to manage them properly in the event of a system component fault. The central issue in FTCS design is how to effectively utilize the redundancy to achieve the robustness against faults.

To evaluate the behavior of a FTCS, we have to develop certain performance measures. These measures should be able to truthfully reflect the system behaviors under the intended operating conditions. These measures can be in time-domain, frequency-domain, or a combination of both. They describe the system behaviors both in the transients as well as during the steady-states.

2.4 Specifications and Performance Measures in FTCS

2.4.1 Three time periods of FTCS

To evaluate the performance of a system and to compare the quality of different designs, a set of performance measures need to be defined. The commonly used performance measures can be classified into two categories: (i) those based on the system input-

output characteristics. Examples are measures of the system responses to some standard test inputs, such as step responses, impulse responses; or some norm-based performance measures, such as mean-square-errors, etc. and (ii) those directly related to the properties of the system itself, e.g. gain and phase margins, eigenstructure, or transfer function characteristics.

From the analysis in Section 2.2, we know that a dynamic system with faults can be modelled as a piecewise time-invariant system. Considering the fact that faults occur only infrequently, it can be assumed that the time between two successive faults is much greater than the largest time constant of the system. The entire operation of the system can be divided into three time periods: pre-fault period, duration of the fault, and post-fault period, as shown in Figure 2.6.

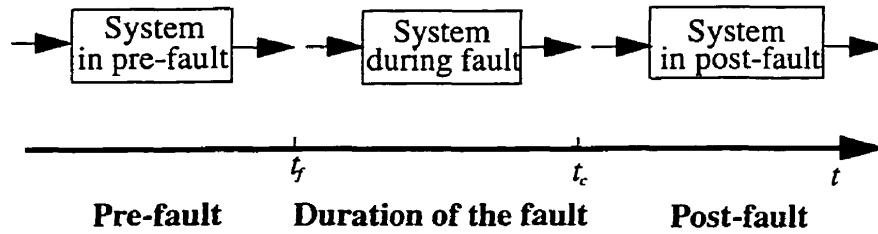


Figure 2.6 Three time periods of system operation in the presence of faults

In this figure, t_f is the time instant at which the fault occurs, and t_c stands for the time instant after which all the transients caused by the fault and the control system reconfiguration have settled down, and the system enters the post-fault period. It is clear that, if the fault is serious and no adequate action is taken against such a fault, then the system may be completely damaged before it enters a post-fault period. This situation is beyond the scope of this thesis.

In the pre-fault and post-fault periods, the system is essentially linear time-invariant. Therefore, various existing performance measures in both time and frequency

domains can be adopted in these two zones. However, the system dynamics in the period from t_f to t_c are more complex. Time-domain based measures should be used because both the evolution of faults and the control system reconfiguration procedure itself (in the case of active FTCS) are time-varying processes. As described in the preceding section, the fault will cause abrupt changes in the system dynamics, which may lead to large transients. In active fault tolerant control systems, the control reconfiguration may also contribute to the variation of the system characteristics. The performance measure in this period should reflect these issues.

2.4.2 *Performance degradation*

In the process of designing passive FTCS, it is possible to select the controller parameters such that the fault-induced transients are minimized for each anticipated fault scenario. The philosophy of graceful degradation in performance should be applied throughout the design to achieve acceptable transient performance for all fault conditions considered.

In an active FTCS, since the exact knowledge of the fault is unknown at the controller design stage, the situation can be much more complex. Once the occurrence of a fault is detected, some preliminary control actions may have to be initiated even with the incomplete knowledge of the fault. As more detailed information on the fault is obtained, improvements on the quality of the control can be made accordingly. Such progressive type of control actions reflects the concept of graceful degradation in an active FTCS design.

Due to the different design philosophies in passive and active FTCS, there are significant difference in the way the performance measures are established in these two approaches. In passive FTCS, the system dynamics under all presumed fault conditions are known *a priori*. Therefore, it is relatively easier to evaluate the system performance for all conceivable fault situations. In active FTCS, the exact knowledge of the fault is

unknown at the controller design stage. Consequently, it is extremely difficult to evaluate the performance of such a system for all possible fault conditions.

To design a passive FTCS, one can assume that there are a set of N presumed fault conditions and the corresponding system dynamics. Together with the fault-free system, there are $(N+1)$ different types of system dynamics that have to be considered. It is often convenient to represent this class of systems by a set of $(N+1)$ multiple models. Since a passive FTCS is designed to cope with all presumed fault conditions, the main objective becomes to ensure that the closed-loop system performs satisfactorily under all $(N+1)$ conditions.

Along with each fault occurrence, the total degree of the system redundancy is reduced, the ability of the system to deal with potential faults decreases as well. As long as the basic system properties, such as the controllability and the observability, are maintained, the primary (high priority) objectives will be achievable in passive FTCS. However, it is not too difficult to imagine that if the number of presumed failure scenarios become too large, it would be more difficult to synthesize a satisfactory controller which works under all conditions. A certain degree of performance degradation would be expected.

2.4.3 *Performance measures for pre-fault and post-fault system operation*

As illustrated in Section 2.4.1, the entire operation of the FTCS system has been divided into three time periods as shown in Figure 2.6. It needs to be pointed that for passive FTCS, because there is no fault detection and no control reconfiguration involved, the duration of the fault totally depends on the transients caused by the fault induced changes in the system. For a well designed passive fault tolerant controller, during the fault period, the fault induced transients should have an acceptable profile. However, one has no control over it once the controller is designed. Therefore, the pre-fault and post-fault performance is extremely important to consider when designing the passive FTCS.

In optimal control based passive FTCS design, the control system is synthesized by minimizing a linear quadratic cost function. A typical format of this function is:

$$J(t) = \int_0^t \{x^T(t) Q x(t) + u^T(t) R u(t)\} dt \quad (2.22)$$

where Q and R are real symmetric positive semi-definite and positive definite matrices, respectively.

The choice of the weighting matrices, $\{Q, R\}$, is different from the those in classical optimal control methods. Further elaboration on the design procedure will be given in Chapter 4. It is important to point out that the values from the above cost function can be evaluated not only for the normal system operation, but also for the system under all conceivable fault conditions. Naturally, the cost function can be served as a measure of the system performance. Since J reflects on the system transients and the control efforts, the minimum value of this cost function will usually correspond to the nominal mode of operation. When a fault occurs, the value of this cost function generally tends to increase. In other words, the degradation in performance has occurred. In the control system design and analysis, it is important to ensure that the value of this cost function is consistently below a certain threshold, [3].

Another group of design methods for passive FTCS is based on eigenvalue assignment. Because faults will inevitably introduce changes in the system dynamics, it will change the eigenvalue locations. A natural measure of the system performance for eigenvalue assignment methods is the relative stability of the system in terms of the locations of the dominant eigenvalues. Under the normal system operation, the real part of the dominant eigenvalues will be in the desired region with a certain minimum distance from the imaginary axis. When a fault occurs in the system, the eigenvalues may move closer towards the imaginary axis. The objective of the passive FTCS is to ensure that all the eigenvalues of the system are on the left side of certain limit. This situation is shown in

Figure 2.7. The distance from the dominant eigenvalues to the imaginary axis is directly related to the relative stability of the system, and can be adopted as a valid measure of the system performance under different fault conditions.

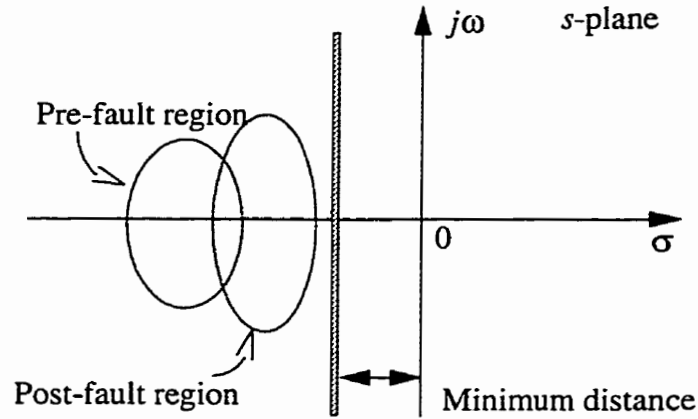


Figure 2.7 Performance degradation in terms of eigenvalue locations

The performance trade-off among various fault conditions can also be examined by using an H_∞ norm of the transfer function matrix between the appropriate system input and output, [4]. The basic idea of this approach is illustrated in Figure 2.8 where the external system input is represented by w and the quantities being controlled is denoted by z .

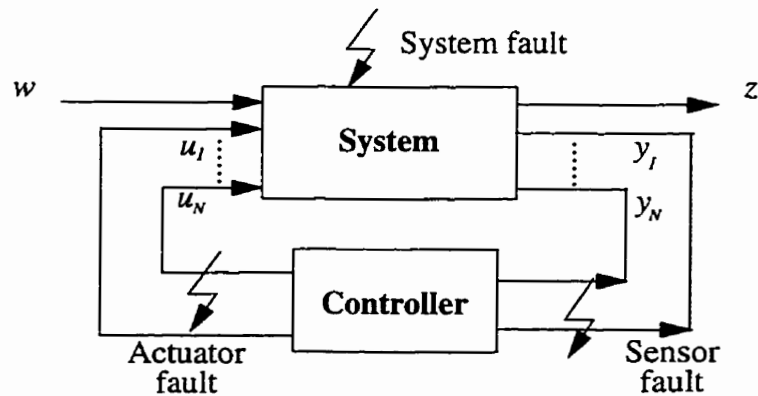


Figure 2.8 H_∞ norm based performance measures

The objective of the control system design is to choose a suitable controller such that the H_∞ norm between w and z is less than a certain value not only during the normal operation but also under various failures:

$$\|T_{zw}(s)\|_\infty \leq \alpha \quad (2.23)$$

where $T_{zw}(s)$ is the transfer function from the input $W(s)$ to the output $Z(s)$.

The actual value of the norm quantity, $\|T_{zw}(s)\|_\infty$, becomes a natural performance measure. As more faults occur in the system, this quantity tends to increase. In other words, it becomes a very valuable indicator for the performance degradation. The value α specifies the performance limit of the system. A similar measure has been used in [5] to balance the robustness of the reconfigurable control system and the sensitivity of the FDI scheme.

As previously mentioned, one conventional way to describe the system is by its transient and the steady-state responses. Therefore, the degradation in performance, in the time-domain, can often be interpreted as a larger overshoot, a slower response, as well as an increased steady-state error, while in the frequency domain, the degradation can be measured in terms of reduced bandwidth, decreased steady-state gain, and the lessened gain/phase margins. The performance of the system is deemed to be acceptable so long as the extent of such degradation is well within the tolerable limits for all presumed fault conditions.

2.4.4 Performance measures for the system during faults

Unlike passive FTCS, for active FTCS, the most crucial period is right after the occurrence of the fault. The performance during this period depends on the severity of the fault and how promptly the control reconfiguration scheme reacts. Generally speaking,

transients are highly undesirable. One of the objectives of active FTCS is to reduce or minimize these transients.

In active FTCS, because the nature and the severity of faults are generally unknown *a priori*, the post-fault system dynamics are not known ahead of time. Fault identification techniques have to be used to construct the post-fault system model for the purpose of control system reconfiguration. The quality of the control will depend on many factors, such as the availability of healthy actuators/sensors, the accuracy of the FDI results, and the type of control strategies adopted in the design. Most of all, there is usually a very limited amount of time available to carry out the post-fault model construction and control reconfiguration. The trade-off among various design objectives has to be carefully considered and conducted on-line in real-time. In this respect, the active FTCS is more complex to design and to implement.

For a given fault scenario, a high peak amplitude of transients (see Figure 2.4) can pose a serious threat to the integrity of the overall system. In practical systems, there always exist certain physical limits on the system variables. Exceeding these limits may have disastrous consequences. In other words, the system variables should stay within the respective bounds at all time.

For a given system, the space in which all the system variables should reside for the integrity of the entire system is defined as the *allowable space*. The actual size of this space depends on the specific application as well as the functional limits of the physical system variables. During the normal system operation, all the system variables are located well within this space. Once a fault has occurred, some system variables may move towards the boundary of this space, and eventually depart from this space if no adequate control actions are carried out. When this happens, we say that a failure has occurred in the system. The amount of time that the system trajectory stays within the allowable space, after the occurrence of a fault, is known as the *hard deadline* [6]. If no appropriate control actions are carried out before this deadline, the total failure of the system becomes immi-

nent. From this point of view, the function of active FTCS is to keep the system trajectory within the allowable space through proper control actions. Obviously, the speed of the control actions is crucial. In this respect, the hard deadline becomes a very important criteria to characterize the severity of the fault as well as a yardstick to measure the effectiveness of the active FTCS. The relationship of the allowable space and the system trajectory is shown in Figure 2.9.

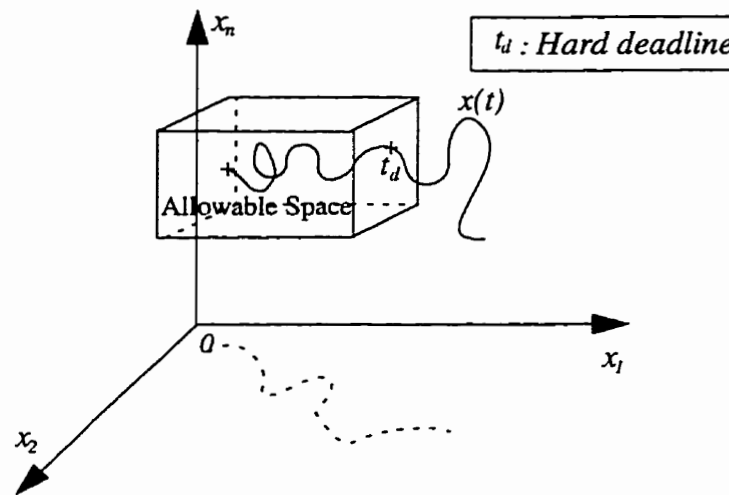


Figure 2.9 The allowable space and the trajectory of the system

For a given system with a set of clearly specified limits on the physical system variables, it is straightforward to define the allowable space. However, the hard deadline will depend not only on the allowable space, but also on the type of faults, the system operating condition when the fault occurs, and the characteristics of the system input following the fault. The way to calculate such a hard deadline highly depends on different applications, and is a challenging problem itself.

2.5 Conclusion

In this chapter, different types of system faults are first modelled in a unified framework. The design objective of FTCS is then elaborated in depth, along with the discussion of performance degradation in FTCS. Finally, the performance specifications for passive and active FTCS are described.

2.6 Bibliography

- [1] K. Suyama, "A new type of reliable control system using decision by majority", *Electronics and Communications in Japan*, Part 2, vol. 81, No. 2, pp. 46 - 54, 1998.
- [2] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*, Prentice Hall, Englewood Cliffs, NJ, 1993.
- [3] R. J. Veillette, "Reliable linear quadratic state-feedback control," *Automatica*, vol. 31, no. 1, pp. 137-143, 1995.
- [4] R. J. Veillette, J. V. Medanic, and W. R. Perkins, "Design of reliable control systems," *IEEE Trans. on Automatic Control*, vol. AC37, No.3, pp. 290-304, 1992.
- [5] N. E. Wu and T. J. Chen, "Feedback design in control reconfigurable system," *International Journal of Control*, vol. 6, pp. 561 - 570, 1996.
- [6] H. Kim and K.G. Shin, "Derivation and application of hard deadlines for real-time control system," *IEEE Trans. on Systems, Man, and Cybernetics*, vol. 22, no. 6, pp. 1403 - 1412, 1992.

Redundancies in Fault Tolerant Control Systems

3.1 Introduction

Redundancy is an important concept in fault tolerant control systems. In fact, one can safely say that: *if there is no redundancy, there will be no fault tolerance*. The redundancy refers to the additional system resources, such as sensors, actuators, or controllers, which are beyond what are needed to achieve the intended control objectives during the normal system operation. Their existence is mainly for combating faults in the system.

In the early days of fault tolerant designs, redundancy was almost always meant to be physical hardware replacements. A rudimentary approach is to use spare parts which can be switched in to replace the faulty elements whenever necessary. In this chapter, the system redundancy is examined from a more fundamental point of view, in terms of its role in maintaining the functional controllability of the system [1] in the event of faults.

The ability of a control system to deal with faults depends mainly on two factors: how much redundancy exists in the system? and, how well such redundancy is being utilized in the presence of failures? It is important to note that the requirements on system reliability and availability play a central role in deciding the degree of redundancy required in the system. A well designed fault tolerant control system with a sufficient amount of redundancies should be able to maintain the basic characteristics and important performance of the system, such as controllability/observability and system stability. As mentioned Chapter 2, the consequence of failures may be reflected as the performance

degradation and a reduction in the total redundancies. Therefore, there exists a close relationship between the fault tolerant capabilities of the system and the amount of redundancy in the system. The higher the degree of redundancy, the more faults that the system is able to handle.

Even though the existence of redundancy is necessary for fault tolerance, it is usually not sufficient, because in order to fully utilize the existing redundancies, effective design techniques have to be developed and employed. In essence, different FTCS design techniques differ in the way that the redundancy is being managed. It is also worthwhile to point out that the whole design process becomes increasingly complex as the degree of the redundancy increases. In practice, the addition of redundant system components is often associated with an increase in the cost, weight, and size from the original system. For a given application, one has to analyze the reliability requirement of the system carefully and decide the right amount of redundancy appropriate for the system.

3.2 Classification of Redundancies

3.2.1 Hardware redundancies

When dealing with redundancy, it is important to differentiate faults in sensors, actuators, or controllers from those occurring in the plant dynamics, because the type of redundancies for these two groups of faults, as well as the ways to compensate for them, are quite different. Since redundant actuators, sensors or controllers are often in hardware forms, this type of redundancy is called hardware redundancy.

A deep understanding of the physical differences between sensors and actuators is important in the modelling and design of FTCS. In a practical system, actuators are often used to manipulate energy flows, mass flows, or to amplify the low-energy control signals to operate a process. They are the devices that mechanically drive the system. Generally speaking, the type and power levels of actuators depend on the specific applications.

Actuators for motion control may include stepper motors, DC servomotors, linear motors, hydraulic or pneumatic motors. In process control industries, actuators can be servo-valves, solenoids, and relays. Since almost all actuators require a separate power source to operate, failures in these power sources will certainly contribute to the failures of the respective actuators. Such failures are often abrupt in nature. In addition, due to the mechanical motions, actuators may also undergo wear or aging. This type of failures manifest themselves as gradual deterioration in the actuator effectiveness.

Similarly, the type of sensors employed is application dependent as well. Potentiometers and linear variable differential transformers are often used to measure linear displacement. Tachometers and accelerometers are used to measure speed and acceleration. Thermocouples, thermistors, or resistance temperature detectors (RTD) are often associated with the temperature measurement. Generally speaking, the signal level at a sensor output is often relatively low. Additional signal conditioning and amplification often become an integral part of the sensory component. Failures in the sensor itself or the related sensor accessories will be classified as sensor failure. The failure profile for sensors is usually different from that for actuators. The predominant problems associated with sensors are bias, loss of power, reduction in the dynamic range, or complete loss of the signal.

For a given system, redundant sensors are usually much easier to install than redundant actuators and controllers, because sensors are passive elements in the sense that they only provide the operational information of the system, and do not affect the system behavior directly (unless they are in the feedback loop). There are several different strategies for introducing redundant sensors. One is to use multiple dissimilar sensors at the same measurement point in the system to obtain multiple readings. These readings are then processed by a majority-voting scheme to discriminate the incorrect reading from reliable ones. A widely accepted reliable measurement strategy in industries is so-called Triple Modular Redundancy (TMR) where three sensors are used to perform the measurement of a single quantity, [2]. Another method is to use different sensors to measure differ-

ent, but related, system variables. Some pre-processing may be required before voting can be carried out, [3].

In comparison with sensors, actuators are larger in size and require significantly more power to operate. In many cases, one cannot ignore the dynamics of the actuators, which are often represented as a part of the entire system. Unlike sensors, they cannot be added or taken out of service easily. Being more precise, the actuator redundancies can only be introduced by means of additional manipulated variables in the system. Furthermore, these redundant system variables may take totally different physical forms or meanings. In other words, the dynamics from each actuator to the system output may be different. Because the redundant actuators have to be in operation at all time, i.e. one can not apply a voting scheme to actuators, the controller design for such systems becomes more complex.

3.2.2 *Analytical redundancies*

Generally speaking, for system dynamic faults, it is more difficult to introduce redundancy in hardware forms. The redundancy in this case is introduced differently, which often reflects the ability of the system to detect and diagnose the component faults, and to reconfigure the control strategies to cope with them. As introduced in Chapter 1, Fault Detection and Identification (FDI) is a very important first step in active FTCS. To achieve prompt fault detection and accurate fault identification, we also have to rely on the redundant information from the system. Such information can be obtained not only from redundant sensors, but also by means of analytical relationships among related system variables. The redundancy derived from a mathematical model is often known as analytical redundancy.

The residual generation schemes of many FDI methods are based on the principle of analytical redundancies. The major hurdle in using analytical redundancy is that one has to have an accurate mathematical model representation among relevant system vari-

ables, which in practice is hard to obtain. This issue brings about a lot of research interests, such as robust FDI, [4], and imprecise FDI for reconfigurable control, [5]. In fact, the control reconfiguration scheme can also be viewed as analytical redundancy, since different (redundant) control strategies are generated and applied to the system in the event of faults/failures. Therefore, analytical redundancy mainly exists in active FTCS. It should be pointed that, even though the analytical redundancy is powerful in many applications, it can not replace redundant hardware components for control purposes. This is particularly true for actuator failures.

3.3 Representation of Redundancies

3.3.1 System structure with hardware redundancies

If one can combine the redundant controllers with the respective redundant actuators and treat them as integrated units, the system hardware redundancy can simply be classified into two types: actuator redundancy and sensor redundancy. In this section, these two type of redundancies are analyzed from a mathematical point of view. The analytical redundancy will be discussed in Chapter 5.

Since the presence of redundant actuators and sensors provides additional system inputs and outputs, the system with actuator/sensor redundancies often appears to be in a multi-variable form. From the basic control point of view, redundant actuators/sensors relate directly to the controllability and observability of the system. To be more precise, for an actuator to be a redundant one, it alone must be able to maintain the complete controllability of the system. Similarly, for a sensor to be a redundant one, it must be able to maintain the complete observability of the system.

To represent the redundancies accurately, one should have a complete understanding of the physical meanings of the related system variables. In fact, the redundancy

analysis is an essential part of any fault tolerant control system design. For this purpose, an anatomical diagram of a system with redundant actuators/sensors is shown in Figure 3.1.

It is clear that, by the nature and locations in the system, redundant actuators provide additional channels for the control signal to reach the system, while redundant sensors merely reflect the duplication of the measured variables. To represent actuators and sensors properly, one has to distinguish the actuator inputs from the system inputs, as well as the system outputs and the sensor outputs. These system quantities are clearly indicated in Figure 3.1. In practice, the system inputs may not always be accessible without appropriate actuators, and the system outputs may not be observed without appropriate sensors. Therefore, we often have to work with the system from the actuator inputs to the sensor outputs.

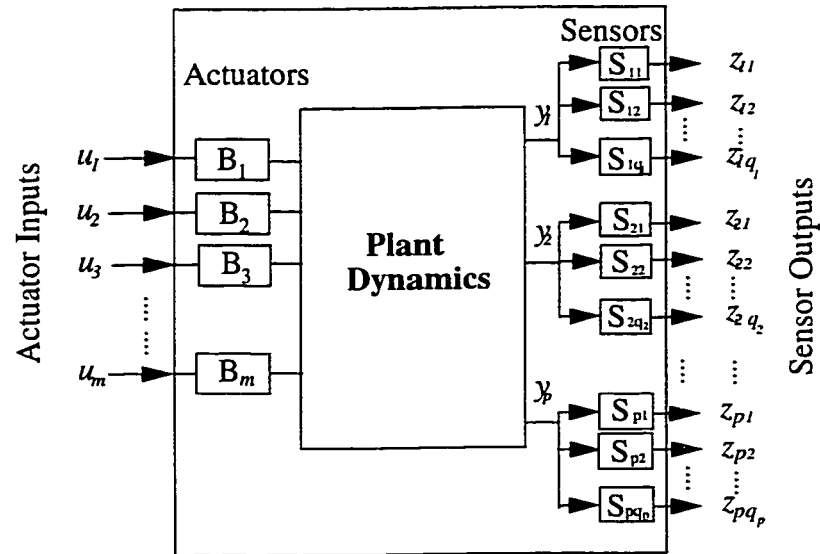


Figure 3.1 A system with multiple actuators and multiple sensors

Assume that the system is described in a state-space representation in EQs (2.1), (2.2) and (2.3), and its transfer function is calculated in EQ (2.6). They are repeated herein for the convenience of reference:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t)\end{aligned}\tag{3.1}$$

and

$$\begin{aligned}Y(s) &= G(s) U(s) \\ G(s) &= C(Is - A)^{-1}B = \{C_i(Is - A)^{-1}B_j, i = 1, 2, \dots, p, j = 1, 2, \dots, m\}\end{aligned}\tag{3.2}$$

Based on Figure 3.1, the sensor outputs can be written as follows,

$$z(t) = My(t) = \begin{bmatrix} \underline{S}_1 & 0 & \dots & 0 \\ 0 & \underline{S}_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \underline{S}_p \end{bmatrix} \begin{bmatrix} y_1(t) \\ y_2(t) \\ \dots \\ y_p(t) \end{bmatrix}\tag{3.3}$$

where $\underline{S}_i, i = 1, 2, \dots, p$, is the redundant sensor gain vector which relates the plant output, y_i , to the sensor output, z_i . Suppose that $\underline{S}_i$ has q_i elements, then $\sum_{i=1}^p q_i = q$.

It is important to emphasize that, in a practical system, the actuators are directly related to the system input matrix B . However, the sensors are related to the measurement matrix M , instead of the output matrix C .

3.3.2 Actuator redundancy

For a dynamic system, more often than not, state controllability alone is not sufficient for certain control objectives, such as regulator and tracking design. Another controllability criteria describing the relationships between the system inputs and outputs, known as functional controllability [1] [6], proves to be useful. Such a concept can also be utilized to define the actuator redundancies.

Definition 3.1 (Functional Controllability)

A system is said to be functionally controllable, if for any given suitable output vector y (defined for $t > 0$), there exists an input vector u (defined for $t > 0$) for which this output vector y can be achieved from the zero initial condition.

Here, “suitable” means that the output vector is sufficiently smooth to be generated without impulse functions in u , and has a Laplace transform, [6]. This definition, in fact, guarantees the independent control of the system inputs over the system outputs. In order to satisfy the functional controllability, the number of inputs must be greater than or equal to the number of outputs, i.e. $m \geq p$.

A necessary and sufficient condition for the functional controllability is illustrated in the following lemma.

Lemma 3.1

- (1) For $m = p$, the system is said to be functionally controllable if and only if the determinant of its transfer function matrix $G(s)$ is non-zero, i.e. $|G(s)| \neq 0$;*
- (2) For $m > p$, the system is said to be functionally controllable if and only if there exists at least one non-zero $p \times p$ minor in the transfer function matrix $G(s)$.*

Based on the system representation in EQ (3.1), and Lemma 3.1, the actuator redundancy can be elaborated in the following definition.

Definition 3.2 (Actuator Redundancy)

The system described in EQ (3.1) is said to possess $(m - p)$ degrees of actuator redundancy if

- (i) the system is completely state controllable;*
- (ii) the number of inputs is greater than the number of outputs, i.e. $m > p$;*

(iii) $\text{rank}[B] \geq p$, and there exist $C_m^p = \frac{m!}{p!(m-p)!}$ non-zero $p \times p$ minors, or in other words, C_m^p non-singular $p \times p$ square sub-matrices in the system transfer function matrix: $G(s) = \{c_j(Is - A)^{-1}b_i, 1 \leq i \leq m; 1 \leq j \leq p\}$.

In the above definition, the first condition guarantees that the system is always stabilizable using the state feedback. The second and third conditions in Definition 3.1 are simply extensions of the concept of functional controllability in the context of actuator redundancy. They guarantee that the system is functionally controllable by any p inputs out of the total m inputs, which simply means that the system has $(m - p)$ degrees of actuator redundancy.

This concept can further be illustrated as follows: for a given $(p \times m)$ transfer function matrix: $G(s)$, let's define two index sets: $I = \{1, \dots, p\}$ and $J = \{j_1, j_2, \dots, j_p\} \subset \{1, \dots, m\}, m > p$. We can form a non-singular $p \times p$ submatrix out of the transfer function matrix denoting it as: $G_{(I, J)}(s)$. Let its complementary set be: $G_{(I, \bar{J})}(s)$. Clearly, $G_{(I, \bar{J})}(s)$ has a dimension of $p \times (m - p)$. If we partition the system input vector accordingly, the system output can be represented as:

$$Y(s) = G_{(I, J)}(s) \cdot U_{(J)}(s) + G_{(I, \bar{J})}(s) U_{(\bar{J})}(s) \quad (3.4)$$

where $U_{(J)}(s)$ and $U_{(\bar{J})}(s)$ are the system input vector partitioned based on the index sets: J and $\bar{J}$.

Clearly, the system output is composed of two parts: the first part is due to the group of p inputs and the second part is due to the remaining $(m - p)$ inputs. In the absence of actuator failures, the first p inputs alone can maintain the functional controlla-

bility of the system. In the presence of an actuator failure within the first group of p inputs, if *any* one of the remaining $(m - p)$ inputs can fill in for the failed actuator, this actuator would be classified as redundancy. Therefore, the system can be said to possess $(m - p)$ degree of actuator redundancy if for any combination of p inputs, i.e. for any $J = \{j_1, j_2, \dots, j_p\} \subset \{1, \dots, m\}$, $m > p$, $G_{(I, J)}(s)$ is non-singular, or the system transfer function matrix $G(s)$ has $C_m^p = \frac{m!}{p!(m-p)!}$ non-zero $p \times p$ minors.

The above definition deals with a situation where any actuator input can be regarded as a redundant input with respect to any system output. For some practical systems, particularly large systems, it may be possible that a certain input can only be considered as a redundant input to a sub-set of the system output. In other words, certain system inputs may be decoupled from certain system outputs. In this case, the actuators associated with the decoupled system inputs can no longer be counted as the redundant actuators for those system outputs. From a mathematical point of view, this situation corresponds to the case where the number of non-zero $p \times p$ minors is less than C_m^p , but greater than one.

Should such a situation arise, it is necessary to decompose the system first. Within the subsystems, the redundant actuators can be identified. One can also think this problem as pairing a group of system inputs with a group of system outputs with the number of inputs more than that of the outputs.

The following example illustrates the concept of the actuator redundancy as defined in Definition 3.2.

Example 3.1 Analyze the degree of actuator redundancy of the system with

$$A = \begin{bmatrix} -1.5 & 1 \\ -0.5 & -2 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (3.5)$$

The transfer function of the above system is calculated as follows:

$$G(s) = \frac{\begin{bmatrix} s+3 & 1 & s+2 & s+3 \\ s+1 & s+1.5 & -0.5 & s+1 \end{bmatrix}}{s^2 + 3.5s + 3.5} \quad (3.6)$$

The minors of this transfer function can be calculated as follows:

$$(1) I = \{1, 2\}, J = \{1, 2\} : |G_{I,J}(s)| = \frac{1}{s^2 + 3.5s + 3.5} \neq 0;$$

$$(2) I = \{1, 2\}, J = \{1, 3\} : |G_{I,J}(s)| = \frac{1}{-s^2 - 3.5s - 3.5} \neq 0;$$

$$(3) I = \{1, 2\}, J = \{1, 4\} : |G_{I,J}(s)| = 0$$

$$(4) I = \{1, 2\}, J = \{2, 3\} : |G_{I,J}(s)| = \frac{1}{-s^2 - 3.5s - 3.5} \neq 0$$

$$(5) I = \{1, 2\}, J = \{2, 4\} : |G_{I,J}(s)| = \frac{1}{-s^2 - 3.5s - 3.5} \neq 0$$

$$(6) I = \{1, 2\}, J = \{3, 4\} : |G_{I,J}(s)| = \frac{1}{s^2 + 3.5s + 3.5} \neq 0$$

The system transfer function only has five non-zero 2×2 minors. As can be seen in case (3) where $J = \{1, 4\}$, input 1 and 4 cannot functionally control either of the two system outputs. Therefore, they cannot be treated as redundant actuators in some cases. For example, in the circumstance of failures of actuator 2 and 3, the system will be paralyzed since actuator 1 and 4 are not able to maintain the functional controllability.

□

Example 3.2 Analyze the degree of actuator redundancies of the system with

$$A = \begin{bmatrix} 1.5 & 1 & 0 & 1.2 \\ 0.5 & 2 & 1 & 0 \\ 0.8 & 0 & 2 & 0.5 \\ 1 & 0 & 0.5 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, C = \begin{bmatrix} 0.2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0.5 \end{bmatrix} \quad (3.7)$$

The transfer function of the above system is obtained:

$$G(s) = \frac{\begin{bmatrix} g_{11}(s) & g_{12}(s) & g_{13}(s) & g_{14}(s) \\ g_{21}(s) & g_{22}(s) & g_{23}(s) & g_{24}(s) \end{bmatrix}}{s^4 + 6.5s^3 + 15.95s^2 + 19.71s + 11.44} \quad (3.8)$$

where

$$\begin{aligned} g_{11}(s) &= 0.2s^3 + 1.5s^2 + 2.25s + 0.28 & g_{21}(s) &= 1.3s^2 + 5.1s + 5 \\ g_{12}(s) &= s^3 + 3.7s^2 + 5.23s + 2.42 & g_{22}(s) &= s^3 + 4.8s^2 + 9.38s + 7.53 \\ g_{13}(s) &= -1.24s^2 - 4.88s - 5.49 & g_{23}(s) &= 1.5s^3 + 8s^2 + 13.61s + 7.26 \\ g_{14}(s) &= -0.24s^2 - 2.06s - 2.05 & g_{24}(s) &= 0.5s^3 + 3.25s^2 + 5.54s + 2.23 \end{aligned} \quad (3.9)$$

It is clear that the above transfer function has totally six($C_4^2 = 6$) non-zero 2×2 minors. Therefore, the system has 2 degrees of actuator redundancies. In other words, any two of the four inputs can control the system, the remaining two can be regarded as redundant ones.

□

In this system, there usually is a manipulated variable associated with each actuator. Different manipulated variables have different physical meanings and often affect the system differently. Therefore, the dynamics of these actuators in different parts of the

system can be totally different. In general, one can distinguish the actuator redundancy into two types: (i) *uniform actuator redundancy*; (ii) *non-uniform actuator redundancy*.

Definition 3.3 (Uniform Actuator Redundancy)

The system described in EQ (3.1) is said to possess $(m - p)$ degrees of uniform actuator redundancy if

(i) the system is completely state controllable;

(ii) the number of inputs is greater than the number of outputs, i.e. $m \geq p$;

(iii) $\text{rank}[B] = p$, and there exist $C_m^p = \frac{m!}{p!(m-p)!}$ non-zero $p \times p$ minors,

or in other words, C_m^p non-singular $p \times p$ sub-matrices in the system transfer

function matrix: $G(s) = \{c_j (Is - A)^{-1} b_i, 1 \leq i \leq m; 1 \leq j \leq p\}$.

The fact that the rank of the B matrix is equal to the number of outputs implies that the dynamics from some inputs to the system states are similar (maybe different by some constant scaling factors). In other words, this condition corresponds to a physical situation where as if some actuators are associated with one single manipulated variable and act on the system at the same input location (or at the symmetric points for symmetrical systems). In this case, overall m actuators act on the system at p different locations. This concept can be seen clearly from Figure 3.2.

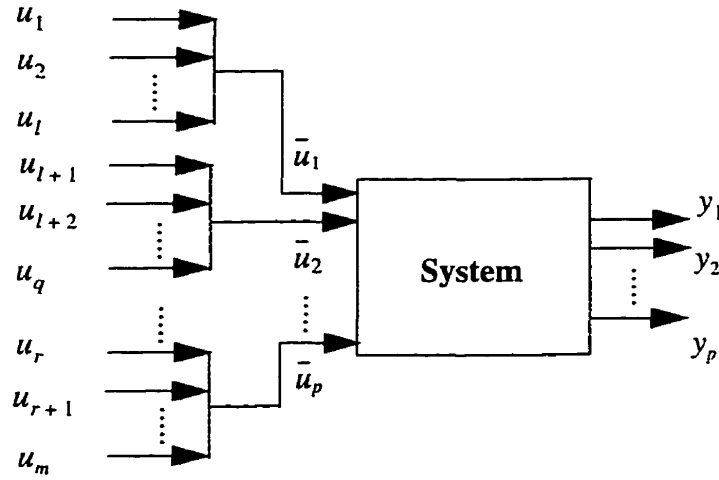


Figure 3.2 Interpretation of the uniform actuator redundancy

In contrast, non-uniform actuator redundancy can be defined as follows:

Definition 3.4 (Non-Uniform Actuator Redundancy)

The system described in EQ (3.1) is said to possess $(m - p)$ degrees of non-uniform actuator redundancy if

(i) the system is completely state controllable;

(ii) the number of inputs is greater than the number of outputs, i.e. $m \geq p$;

(iii) $\text{Rank}[B] > p$, and there exist $C_m^p = \frac{m!}{p!(m-p)!}$ non-zero $p \times p$ minors,

or in other words, C_m^p non-singular $p \times p$ sub-matrices in the system transfer

function matrix: $G(s) = \{c_j(Is - A)^{-1}b_i, 1 \leq i \leq m; 1 \leq j \leq p\}$.

Such an input matrix B implies that different actuators act on the system from different locations in the system. The control signals passing through these actuator chan-

nels often affect the system differently. This is a general characteristics of a physical system with dissimilar actuators.

Experience has shown that design of FTCS, particularly certain passive FTCS, becomes much easier if the actuator redundancy is of the uniform type. It is important to realize that this type of redundancy exists only in very idealized situations. In practice, few systems possess such a nice property. Fortunately, for most practical systems, we can convert the *non-uniform* actuator redundancy to a *uniform* one by using a properly designed dynamic pre-compensator. The detailed procedure of designing this pre-compensator will be described in Chapter 4.

3.3.3 Sensor redundancy

Unlike redundant actuators which can affect the entire system, the concept of redundant sensors relates only to a single system output at a time. In general, there is no direct coupling among sensors for different system output. It is not the system output matrix, but the measurement matrix which dictates the amount of sensor redundancy in the system.

Definition 3.4 (Sensor Redundancy)

The system described in EQs (3.1) & (3.3) is said to possess $(q_i - 1)$ degrees of sensor redundancy associated with the plant output y_i , if there are q_i non-zero elements in the vector $\underline{S}_i$ in EQ (3.3).

It is clear that in the absence of sensor redundancy, $q_i = 1$, and $q = p$, $M = I_{p \times p}$, where $I_{p \times p}$ is a $p \times p$ identity matrix.

Example 3.3 For a multi-output system, suppose that the sensor and the system outputs are governed by the following measurement equation:

$$z(t) = \begin{bmatrix} z_{11} \\ z_{12} \\ z_{13} \\ z_2 \\ z_{31} \\ z_{32} \end{bmatrix} = My(t) = \begin{bmatrix} s_{11} & 0 & 0 \\ s_{12} & 0 & 0 \\ s_{13} & 0 & 0 \\ 0 & s_{21} & 0 \\ 0 & 0 & s_{31} \\ 0 & 0 & s_{32} \end{bmatrix} \begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} \quad (3.10)$$

It becomes obvious that there are two redundant sensors for the system output, y_1 , no redundancy for y_2 , and one redundant sensor for y_3 .

In the case of sensor redundancies, it is possible to generate additional information on the desired plant outputs through other intermediate state variable. This type of scheme is referred to as *hybrid redundant sensors*. By hybrid, we mean that both the physical redundant sensors and the analytical models are used to obtained the system outputs. An illustrative diagram for this hybrid redundant sensor scheme is shown in Figure 3.3.

There are several distinctive advantages to the hybrid type of redundancy: (i) since the desired system output is derived by measuring other intermediate variables, one has more freedom to choose system variables which are easier to access or more reliable to measure; and (ii) redundant sensors can be used to measure those intermediate system variables as well.

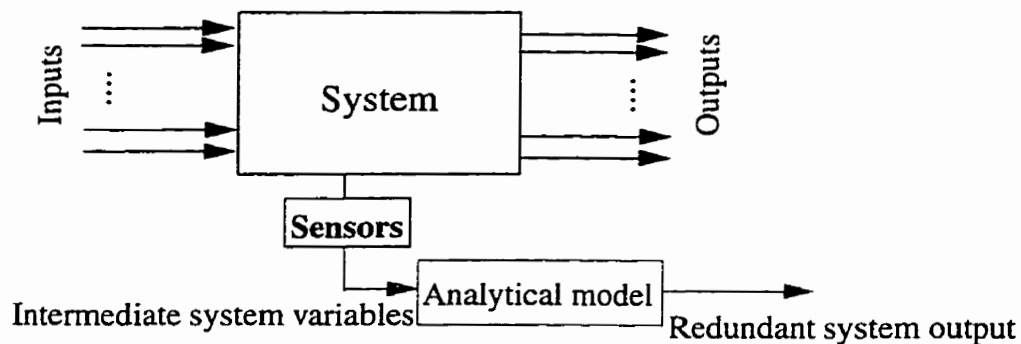


Figure 3.3 Hybrid redundant sensors

In comparison with analytical redundancies, the redundancies considered above are all in the form of extra physical elements (hardware redundancy). The basic idea of analytical redundancy is to compare the behavior of the system against that predicted by the mathematical model of the system. Any discrepancy would lead to an alarm for the occurrence of the fault. However, it is important to realize that, in most cases, analytical redundancies cannot replace physical redundancies. This is particularly true in actuators because even though the mathematical model may provide the desired information, it will never be able to deliver the necessary power needed in the actuator channel. In fact, analytical redundancy is meant only to provide necessary information for the purpose of fault detection and identification.

3.4 Conclusion

In this chapter, the important concept of the system redundancy has been explored in depth. Definitions of actuator and sensor redundancies are introduced and elaborated with the emphasis on their physical meanings.

3.5 Bibliography

- [1] H. H. Rosenbrock, *State Space and Multivariable Theory*, London, Nelson, 1970.
- [2] K. Suyama, "A new type of reliable control system using decision by majority", *Electronics and Communications in Japan*, Part 2, vol. 81, no. 2, pp. 46 - 54, 1998.
- [3] Q. Zhao, J. Jiang and P. E. Orban, "Reliable servo system design with redundant sensors," in *Sensors and Controls for Intelligent Machining, Agile Manufacturing, and Mechatronics*, P. F. Muir and P. E. Orban, Editors, *Proceedings of SPIE (The International Society of Photo-Optical Instrumentation Engineers)*, vol. 3518, pp. 66-72, 1998.
- [4] R. Patton, P. Frank and R. Clark, *Fault Diagnosis in Dynamic Systems, Theory and Application*, edited, Prentice Hall Ltd., UK, 1989.
- [5] J. Jiang and Q. Zhao, "Reconfigurable control based on imprecise fault identification," *Proceedings of 1999 American Control Conference*, June 2-4, San Diego, U.S.A, pp. 114-118, 1999.
- [6] R. V. Patel and N. Munro, *Multivariable System Theory and Design*, International series on *Systems and Control*, Volume 4, Pergamon Press, pp. 40 - 41, 1981.
- [7] R. W. Brockett and M. D. Mesarovic, "The reproducibility of multivariable systems," *Journal of Math. Anal. Appl.*, vol. 11, pp. 548 - 563, 1965.

Design of Passive Fault Tolerant Control Systems[†]

4.1 Introduction

As first introduced in Chapter 1, a passive fault tolerant control system is a control system designed to tolerate system component failures with acceptable performance degradation, without changing the control strategy or parameters. Such systems are also referred to as reliable control systems in the literature, [1], or control systems with integrity, [2]. One of the advantages of properly designed passive FTCS is that the robustness against component failures has already been built into the system. In other words, the fault scenarios have already been taken into account at the controller design stage. However, the design procedure for such controllers is often more involved because the control system has to perform satisfactorily not only during normal system operation but also under various component failures. In this chapter, some of the existing design techniques are briefly reviewed, then newly developed design techniques for passive FTCS against actuator and sensor failures are elaborated with examples.

[†]: Some material in this chapter has been published in *Automatica, Journal of IFAC (International Federation of Automatic Control)*, vol. 34, no. 10, pp. 1267 - 1272, 1998: Q. Zhao and J. Jiang, "Reliable state feedback control system design against actuator failures."

4.2 Review of the Existing Passive FTCS Design Techniques

4.2.1 *The concept of system integrity and related work*

From Chapter 1, one has learned that, in the development of passive fault tolerant control systems, the concept of system integrity from multivariable system theory has played a very important role and has become one of the main design objectives. Some of the early research work in the area of passive FTCS synthesis has focussed on the maintenance of system integrity.

The concept of system integrity was first introduced in [3] and further elaborated in [4] by MacFarlane. In multivariable systems, the interaction among different loops makes the control systems design more difficult, and when there are failures in some loops, the interaction among the remaining loops may result in the reduction of the system stability margins. Such a problem brought up the question of system integrity. A multivariable feedback system is said to have “high integrity” if it remains stable under all likely failures. Here, all “likely” failures mean all types of loop failures, such as output transducer, controller and actuator failures.

Based on the defined system return-ratio matrices and the traditional Nyquist stability criteria, some necessary and sufficient conditions on system integrity are given in [4]. Inspired by this work, more results have been obtained on conditions of system integrity. A notable one is by Fujita and Shimemura, [5]. By introducing a new class of matrices called the U-matrix, necessary and sufficient conditions for integrity are derived and some previous conditions are unified and extended.

Based on this new concept, some conventional control techniques have been re-examined in the context of MIMO control system possessing integrity. These approaches are briefly reviewed in this section.

1. Methods based on Riccati-type equations and Lyapunov functions

A design method for linear systems possessing integrity using state-feedback control was proposed by Shimemura and Fujita in [2]. The state-feedback gain is chosen based on the solution of a Riccati-type equation.

For a linear time-invariant system given in EQ (2.1), with the actuator failure defined in a so-called switching matrix, L_a , which is similarly defined as in EQ(2.14), the system state equation then becomes:

$$\dot{x}(t) = Ax(t) + BL_a u(t) \quad (4.1)$$

where $x \in \mathfrak{R}^n$, $u \in \mathfrak{R}^m$ are the system state and input vectors, respectively, and the matrices, A, B , are of appropriate dimensions.

It is assumed in [2] that (A, B) is controllable and the open-loop system is asymptotically stable. A Riccati-type equation can then be defined as

$$P_r A + A^T P_r + P_r B R_r^{-1} B^T P_r + Q_r = 0 \quad (4.2)$$

where Q_r and R_r are $n \times n$ and $m \times m$ real symmetric positive semi-definite and positive definite matrices, respectively. If the matrix function

$$F(s, Q_r, R_r) = R_r - B^T (-sI - A^T)^{-1} Q_r (sI - A)^{-1} B \quad (4.3)$$

is positive semi-definite for all $s = j\omega$, i.e. $F(j\omega, Q_r, R_r) \geq 0$, $\omega \in \mathfrak{R}^{1 \times 1}$, then there exists a positive semi-definite solution to EQ (4.2), $P_r \in \mathfrak{R}^{n \times n}$.

The state-feedback control law can be obtained as:

$$u(t) = -B^T P_r x(t) \quad (4.4)$$

Such a controller can be proved to be able to maintain the asymptotic stability of the closed-loop system, i.e.

$$\text{Re} \{ \lambda [A - BL_a B^T P_r] \} < 0 \quad (4.5)$$

for all possible combination of L_a .

In addition, in the case of normal operation, i.e. $L_a = I_{m \times m}$, where $I_{m \times m}$ is an identity matrix of dimension $m \times m$, the closed-loop system with the above state-feedback is optimal with respect to the following performance index:

$$J_r = \int_0^\infty \{ x^T(t) [P_r B (I + R_r^{-1}) B^T P_r + Q_r] x(t) + u^T(t) \cdot I \cdot u(t) \} dt \quad (4.6)$$

Furthermore, in addition to the system integrity, by taking into account of other dynamic characteristics, a schematic design procedure for choosing an appropriate matrix R_r is developed in [2] to assign the dominant eigenvalues of the system to a desired region, which is circumscribed by a hyperbola in the left-half s -plane.

Enlightened by the above research, similar works were carried out by solving a matrix Lyapunov function in [6] instead of a matrix Riccati-type equation.

Based on the same system model as EQs (4.1), a Lyapunov function is used:

$$A^T P_l + P_l A + Q_l = 0 \quad (4.7)$$

where $Q_l \in \mathbb{R}^{n \times n}$ is a real symmetric positive semi-definite matrix.

By solving the above function, a state-feedback control law can then be applied to the system:

$$u(t) = -\gamma B^T P_l x(t) \quad (4.8)$$

where P_l is the real symmetric nonnegative matrix, which is the solution of EQ (4.7), and $\gamma > 0$ is a constant.

It has been shown that, with this state-feedback, the closed-loop system remains stable despite actuator failures, as long as the open-loop system is asymptotically stable. Meanwhile, the following performance index is minimized for the normal system:

$$J_l = \int_0^\infty \{ x^T(t) [\gamma(Q_l + \gamma P_l B B^T P_l)] x(t) + u^T(t) \cdot I \cdot u(t) \} dt \quad (4.9)$$

Furthermore, an iterative design procedure has been proposed, not only to guarantee the stability, but also to assign eigenvalues of the closed-loop system to the desired stability region, even in the presence of actuator failures. In this design procedure, the main concern is how to choose the positive matrix Q_l , and the constant γ properly. Certain conditions have been developed for this purpose.

Compared to [2], a more general eigenvalue region is used in [6], and the design procedure is iterative and more applicable. However, there is the strong assumption of open-loop system stability in both works. Otherwise, there is no guarantee of system stability under system actuator failures for the proposed methods. In other words, these methods cannot be used for open-loop unstable systems.

2. Methods based on Linear Quadratic Regulator (LQR) Design

It is well known that the linear-quadratic state-feedback regulator has nice robustness properties including an infinite gain margin and a 50% gain-reduction tolerance, [7]. Therefore, such a property has drawn some research interest and has been

applied to the design of a linear quadratic regulator that can guarantee stability and a certain level of performance despite control loop failures. In [8], the design of reliable controllers for multivariable systems has been considered in this framework. In the proposed method, the system does not have to be open-loop stable. A sufficient condition for the system stability under actuator failures was developed.

Figure 4.1 depicts the structure of the reliable control system in [8]:

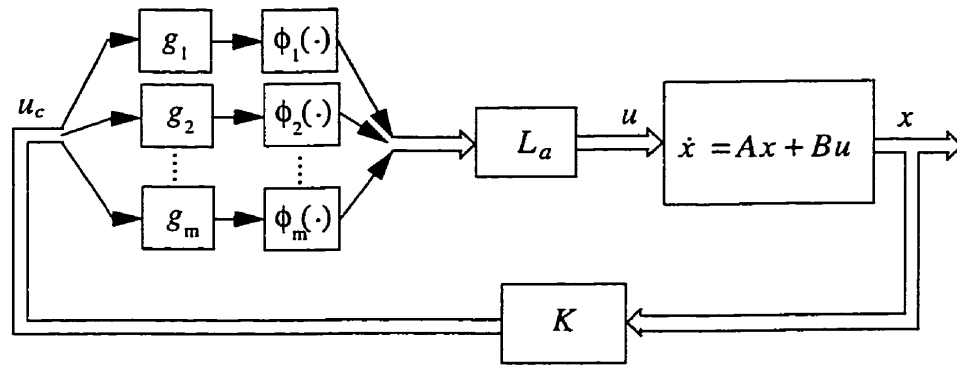


Figure 4.1 The reliable control system structure using LQR design

Similarly, the failure is modelled in the diagonal matrix L_a as defined in EQ (2.7), where I_k , $k=1, 2, \dots, 2^m-1$ denote the set of indices corresponding to the failed actuator. The actuator non-linearity is modelled in $\phi(\cdot)$, which is assumed belonging to the $[\mu_i, \infty)$ sector (i.e. $\sigma\{\phi(\sigma) - \mu_i\sigma\} \geq 0$ and $\phi(0) = 0$), and g_i , $i=1, 2, \dots, m$, are gains in the actuator channels. The closed-loop system equation then becomes:

$$\begin{aligned} \dot{x} &= Ax + BL_a \phi(Gu_c) \\ G &= \text{diag}(g_1, g_2, \dots, g_m) \end{aligned} \quad (4.10)$$

The state-feedback control law is chosen as:

$$u(t) = -R_o^{-1} B^T P_o x(t) \quad (4.11)$$

so that $J_o = \int_0^\infty e^{2\alpha t} (x^T Q_o x + u^T R_o u) dt$ is minimized, where $\alpha \geq 0$ is a constant, R_o is assumed to be a diagonal symmetric definite matrix, and Q_o is a symmetric semi-definite matrix except for $\alpha=0$ ($Q_o > 0$ if $\alpha=0$). The matrix P_o in EQ (4.11) is the solution of the following Riccati equation:

$$A^T P_o + P_o A + 2\alpha P_o - P_o B R_o^{-1} B^T P_o = -Q_o \quad (4.12)$$

With the above control law, even under the actuator failure, the closed-loop system will remain asymptotically stable as long as the following condition is satisfied:

$$Q_o + 2\alpha P_o + P_o B R_o^{-1} [LE - (I - L)] B^T P_o > 0 \quad (4.13)$$

where E is defined as: $E = \text{diag}(e_1, e_2, \dots, e_m)$, $e_i = 2\mu_i g_i - 1$. The above condition depends on the system input matrix B and other parameters, such as, Q_o , R_o , α and P_o .

It should be noted that the above design procedure cannot tolerate all possible $2^m - 1$ cases of actuator failures, but rather only a subset of them. This can be seen clearly through the investigation conducted below.

Noticed from EQ (4.13) that this condition can be guaranteed if the following is true:

$$\tilde{B} [LE - (I - L)] \tilde{B}^T \geq 0 \quad (4.14)$$

where $\tilde{B} = B R_o^{-1/2}$.

Let $B = \begin{bmatrix} B_1 & B_2 \end{bmatrix}$, in which B_1 denotes the $n \times m_1$ submatrix corresponding to the healthy actuators, while B_2 denotes the $n \times (m - m_1)$ submatrix corresponding to the

failed ones. Similarly, one can have $\tilde{B} = [\tilde{B}_1 \ \tilde{B}_2]$, $L = \begin{bmatrix} I_{n \times m_1} & 0_{n \times (m-m_1)} \end{bmatrix}$, and $E = \begin{bmatrix} E_1 & E_2 \end{bmatrix}$. By a simple mathematical manipulation, it can be obtained that:

$$\tilde{B} [LE - (I - L)] \tilde{B}^T = \tilde{B}_1 E \tilde{B}_1^T - \tilde{B}_2 \tilde{B}_2^T \quad (4.15)$$

For this matrix to be non-negative, it can be derived that the columns of $\tilde{B}_2$ must be spanned by those of $\tilde{B}_1$, or in other words,

$$\text{range}(B_2) \subseteq \text{range}(B_1) \quad (4.16)$$

This condition simply implies that only certain subset of actuator failures can be tolerated, rather than all possible failure modes.

It should be mentioned that this design method considers more practical control problem (actuator/sensor failure and nonlinearity) and relieves the constraint of open-loop system stability. However, only failures of a subset of actuators can be tolerated in the proposed method, and other system performance has not been considered.

In 1995, Veillette proposed a design method, which is also LQR based, but with the consideration of optimal system performance under system actuator failures, [9]. Similarly, the modes of actuator failures have been restricted to a subset of actuators.

Based on the system model in EQ (2.1), without loss of generality, the input matrix can be written in the following form:

$$B = \begin{bmatrix} B_{\Omega} & B_{\Omega'} \end{bmatrix} \quad (4.17)$$

where Ω denotes the subset of actuators subject to failures, and the complementary subset Ω' contains the functional actuators.

Correspondingly, the state feedback gain and the matrix R_v in the Ricatti equation are written as the following forms:

$$K_v = \begin{bmatrix} K_{\Omega'} \\ K_{\Omega} \end{bmatrix}, R_v = \begin{bmatrix} R_{\Omega'} & 0 \\ 0 & R_{\Omega} \end{bmatrix} \quad (4.18)$$

By solving the following Ricatti equation:

$$A^T P + P A - P B_{\Omega} R_{\Omega'}^{-1} B_{\Omega'}^T P + Q_v = 0 \quad (4.19)$$

the stabilizing solution P_v depends on the inputs related only to the functional actuators in Ω' .

Choosing $K_{\Omega'} = -R_{\Omega'}^{-1} B_{\Omega'}^T P_v$, and $K_{\Omega} = -R_{\Omega}^{-1} B_{\Omega}^T P_v$, one can have:

$$K_v = \begin{bmatrix} K_{\Omega'} \\ K_{\Omega} \end{bmatrix} = -R_v^{-1} B^T P_v \quad (4.20)$$

It should be noted that the above design is equivalent to a standard LQR design with a state weighting matrix $\tilde{Q} = Q_v + P_v B_{\Omega} R_{\Omega}^{-1} B_{\Omega}^T P_v$, because by a simple manipulation of EQ (4.19), one has:

$$A^T P_v + P_v A - P_v B R_v^{-1} B^T P_v + \tilde{Q} = 0 \quad (4.21)$$

Therefore, the above controller can guarantee system stability even under the occurrences of a presumed subset of actuator failures, i.e. Ω . At the same time, the following cost function can be minimized:

$$J_v = \int_0^{\infty} \left(x^T \tilde{Q} x + u^T R_v u \right) dt \quad (4.22)$$

In the case of failures in all actuators within Ω , this cost function becomes:

$J = \int_0^\infty (x^T Q_v x + u_\Omega^T R_\Omega u_\Omega) dt$. Therefore, the reliable LQ regulator designed in [9] guarantees both stability and performance. One condition for the existence of a reliable controller is that (A, B_Ω) is stabilizable. Compared to the conditions given in [8], the above design procedure is simpler and the conditions are much milder.

In summary, based on the LQR design, a reliable controller protecting against component failures, especially actuator failures, can be well achieved under the condition that only a certain subset of actuators are subjected to failures. It is impossible for such methods to deal with failures in any number of actuators.

4.2.2 *Methods based on decentralized/centralized control*

In the preceding sections, the reliable control design process is to synthesize a single controller to stabilize the multivariable system under different loop failure modes in the context of system integrity.

Inspired by von Neumann's idea for building a reliable computer, a multiple control system structure was proposed by Siljak in the context of decentralized control for complex systems [10] [11]. The essential concept of redundancy has been introduced in the form of parallel connection of multiple controllers. It should be mentioned that, although it was not explicitly defined or modelled mathematically, the idea of redundancy in Siljak's work is believed to be a very original one in a control system framework. Along with the development of fault tolerant control systems design techniques, the concept of redundancy has evolved diversely, and has been employed in a variety of applications.

Figure 4.2 and Figure 4.3 depict generic structures of centralized and decentralized control with possible failures, proposed in [11]:

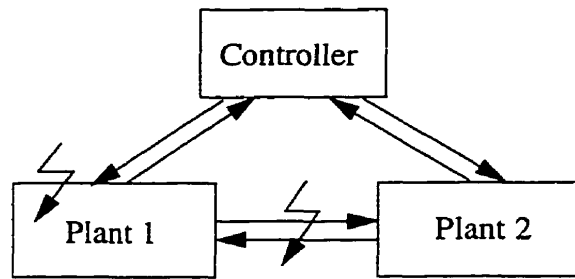


Figure 4.2 Centralized control with plant failures

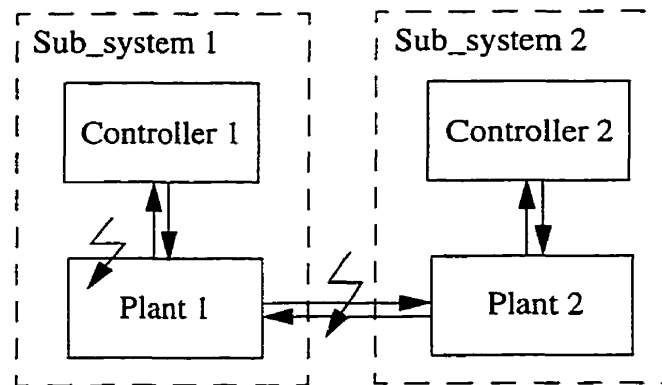


Figure 4.3 Decentralized control with plant failures

The plant failures can further be distinguished into failures of interconnections among the subplants and failures of the subplants themselves (they are modelled as the total disconnection of failed subplants from the rest of the system). It has been demonstrated in [11] that by designing a decentralized control system properly, such a plant failure can be tolerated. In a control system, partial or total controller failures may also occur, that is either the connection between the controller and the subplant fails or the entire controller is disconnected from the plant. Under such circumstances, both the centralized and decentralized control structure cannot guarantee fault tolerance. Therefore, a multiple control system structure was proposed for this purpose, which is shown in Figure 4.4. In this structure, the redundancy is introduced by assigning more controllers to the plant, so that

the reliability of the whole system can be improved. This can be seen clearly by the following reliability analysis.

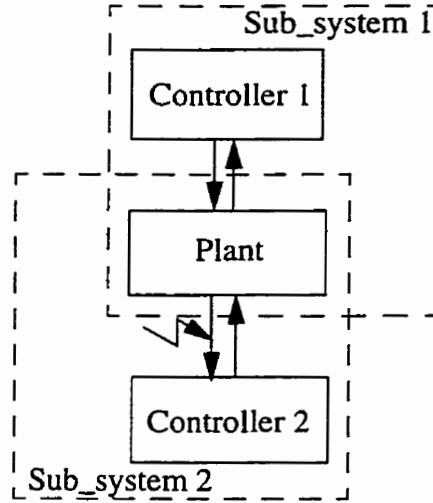


Figure 4.4 Multiple control system with controller failures.

Assign a binary number to each controller:

$$c_i = \begin{cases} 1 & \text{the } i\text{th controller is operational} \\ 0 & \text{the } i\text{th controller has failed} \end{cases} \quad (4.23)$$

where $i \in P = \{1, 2, \dots, P\}$, P is the number of controllers. The assumption in EQ (4.23) is an idealization of the practical situation for the purpose of simplicity, since usually the controller can cover a continuous range of operational modes, rather than covering only a *binary* operation.

Another binary indicator is associated with the whole control system:

$$\varphi = \begin{cases} 1 & \text{the } i\text{th control system is operational} \\ 0 & \text{the } i\text{th control system has failed} \end{cases} \quad (4.24)$$

Here, “operational” means that the overall plant is covered by a controller. For a series control structure, as shown in Figure 4.3, the state of the control system is then given as:

$$\varphi = \varphi(c) = c_1 c_2 = \min \{c_1, c_2\} \quad (4.25)$$

In the case of M controllers in series, from EQ (4.24), the whole control system has:

$$\varphi(c) = \prod_{i=1}^M c_i = \min \{c_1, c_2, \dots, c_M\} \quad (4.26)$$

Therefore, it can be seen that the reliability of the whole system depends on the least reliable controller. Hence, such a control structure is not fault tolerant to the controller failure. The multiple control system in Figure 4.4 has a parallel structure, and for M controllers in parallel, the state of the whole system is obtained as:

$$\varphi(c) = 1 - \prod_{i=1}^M (1 - c_i) = \max \{c_1, c_2, \dots, c_M\} \quad (4.27)$$

In this case, the reliability of the whole system depends on the most reliable controller, in other words, the overall control system is operational as long as there is one nominal controller.

In order to design the controller, the following model of the multiple control system in Figure 4.4 is considered:

$$\begin{aligned} \text{Controller 1: } \dot{x}_1(t) &= A_{11}x_1(t) + A_{12}x_2(t) + B_1u_1(t) \\ \text{Plant: } \dot{x}_2(t) &= A_{21}x_1(t) + A_{22}x_2(t) + A_{23}x_3(t) \\ \text{Controller 2: } \dot{x}_3(t) &= A_{32}x_2(t) + A_{33}x_3(t) + B_2u_2(t) \end{aligned} \quad (4.28)$$

where $x_1(t) \in \mathbb{R}^{n_1 \times 1}$, $x_2(t) \in \mathbb{R}^{n_2 \times 1}$, $x_3(t) \in \mathbb{R}^{n_3 \times 1}$ are states of controller 1, the plant and controller 2; and $u_1(t)$, $u_2(t)$ are the inputs to the respective controllers. The above equation can also be written in the following form:

$$\begin{aligned} S: \dot{x}(t) &= Ax(t) + Bu(t) \\ A &= \begin{bmatrix} A_{11} & A_{12} & 0 \\ A_{21} & A_{22} & A_{23} \\ 0 & A_{32} & A_{33} \end{bmatrix} \quad B = \begin{bmatrix} B_1 & 0 \\ 0 & 0 \\ 0 & B_2 \end{bmatrix} \end{aligned} \quad (4.29)$$

where $x(t) = [x_1^T(t) \ x_2^T(t) \ x_3^T(t)]^T$. Then the system S can be expanded into the following form:

$$\begin{aligned} \tilde{S}: \quad \dot{\tilde{x}}_1(t) &= \tilde{A}_1 \tilde{x}_1(t) + \tilde{B}_1 u_1(t) + l_{12} \tilde{A}_{12} \tilde{x}_2(t) \\ \dot{\tilde{x}}_2(t) &= \tilde{A}_2 \tilde{x}_2(t) + \tilde{B}_2 u_2(t) + l_{21} \tilde{A}_{21} \tilde{x}_1(t) \end{aligned} \quad (4.30)$$

where $\tilde{x}_1(t) = [x_1^T(t) \ x_2^T(t)]^T$, and $\tilde{x}_2(t) = [x_2^T(t) \ x_3^T(t)]^T$. l_{12} and l_{21} are the two binary indicators which equal to 1s when the controllers are functioning properly and otherwise equal 0s. By writing

$$E = \begin{bmatrix} 0 & l_{12} \\ l_{21} & 0 \end{bmatrix} \quad (4.31)$$

it is clear that the multiple control structure in Figure 4.4 has three configurations of interests:

$$E_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad E_2 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad E_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad (4.32)$$

E_1 indicates the normal operation of the system, E_2 and E_3 indicate the controller failure case, i.e. one of the two controllers is completely disconnected from the plant. Then the reliable control design problem is reduced to stabilizing $\tilde{S}$ in EQ (4.30) under the structural perturbations in EQ (4.32). By choosing the control law as:

$$u_1(t) = -\tilde{K}_1 \tilde{x}_1(t), u_2(t) = -\tilde{K}_2 \tilde{x}_2(t) \quad (4.33)$$

The closed-loop system can be obtained as:

$$\begin{aligned} \tilde{S}_c: \dot{\tilde{x}}(t) &= \tilde{A}_c(L) \tilde{x}(t) \\ \tilde{A}_c &= \begin{bmatrix} \tilde{A}_1 - \tilde{B}_1 \tilde{K}_1 & l_{12} \tilde{A}_{12} \\ l_{21} \tilde{A}_{21} & \tilde{A}_2 - \tilde{B}_2 \tilde{K}_2 \end{bmatrix} \end{aligned} \quad (4.34)$$

The reliable control system can then be achieved by choosing $\tilde{K}_1$ and $\tilde{K}_2$ so that the $\tilde{S}_c$ under the three control structures are stable. Therefore, the reliable control system design using multiple controllers can finally be reduced to the simultaneous stabilization problem, [12], which is concerned with finding a single controller to stabilize simultaneously each member of a family of plants. One can think of a family of plants as various operations of a single plant subject to structural perturbations or controller failures.

The design of reliable centralized and decentralized control systems has further been investigated in an unified framework in [1]. The designed control system will only provide guaranteed system stability, and also optimize performance in an H_∞ sense, in both normal and component failures cases. The constraint for this method is that failures can only occur among a prespecified subset of system components. One of the contributions of the method is that it provides a way to measure of the performance of designed reliable control system in terms of a H_∞ norm bound. This has also been discussed in Sec-

tion 2.3.3, where different measures of performance degradation are introduced. This design approach has been extended to discrete-time systems in [13].

4.2.3 Methods based on regional eigenvalue assignment

Since the reliable control problem can be viewed as a problem of robust control against system component failures, the solution of reliable control can also be found using some robust techniques, such as the regional pole assignment technique in parametric space, which has been illustrated in detail in [14] and [15]. A graphical approach has been proposed in [15] to select stabilizing state-feedback gains. An example is given to show how to design a reliable state-feedback controller against possible sensor failures. The problem can be briefly stated as follows:

With the following system model and the control law:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) \\ u(t) &= -Kx(t) + v\end{aligned}\tag{4.35}$$

If one can specify a set of eigenvalues, $s_1, s_2, \dots, s_n$, the characteristic polynomial of the closed-loop system can be written as the following factorized form:

$$p(s) = \det(sI - A + BK) = (s - s_1)(s - s_2) \dots (s - s_n)\tag{4.36}$$

K can be chosen to assign the closed-loop eigenvalues to the desired locations, i.e. $s_1, s_2, \dots, s_n$. Standard eigenvalue assignment techniques can be used to solve K . For the single input systems, one can simply use Ackermann's formula:

$$K = e^T (A - s_1 I) (A - s_2 I) \dots (A - s_n I)\tag{4.37}$$

where $e^T = [0 \dots 0 \ 1] [B \ AB \ \dots \ A^{n-1}B]^{-1}$. Such a state-feedback will assign closed-loop system eigenvalues to the specified locations.

The problem as described above is a standard eigenvalue assignment problem. Since the occurrence of faults will alter the system dynamics, it is impossible to assign eigenvalues to fixed locations. Rather, a desired region in the left half of the s -plane is more suitable for the design specifications. Such a region is often called the Γ -stability region, [15]. It has a boundary that consists of several contours in the s -plane, such as straight line, hyperbolae, circular arcs, and so on. Usually the boundary is chosen according to the desired system stability margin, damping, and bandwidth limit. Figure 4.5 shows a typical Γ -stability region:

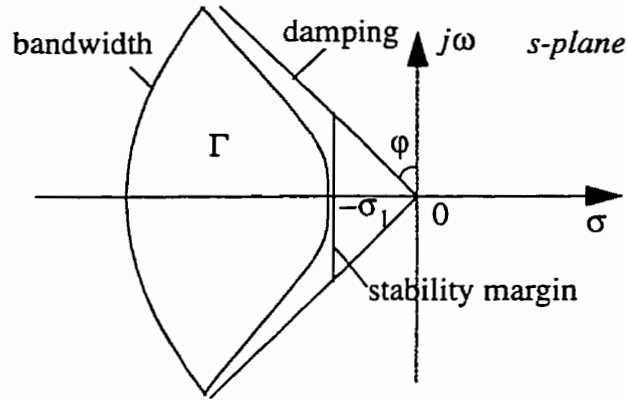


Figure 4.5 A Γ -stability region

Therefore, instead of specifying eigenvalue locations, based on such a Γ -stability region, the designed feedback gain should be robust to parameter changes. In this case, the solutions of EQ (4.37) forms an admissible set of feedback gains K_Γ such that:

$$\{s_1, s_2, \dots, s_n\} \in \Gamma \Leftrightarrow K \in K_\Gamma \quad (4.38)$$

Using the above regional eigenvalue assignment technique, the simultaneous stabilization of a family of plants, (A_i, B_i) , $i = 1, 2, \dots, N$, can be solved just by finding the following intersection:

$$K_{\Gamma} = \bigcap_{i=1}^N K_{\Gamma}^{(i)} \quad (4.39)$$

where $K_{\Gamma}^{(i)}$ is the admissible set of feedback gains corresponding to the system (A_i, B_i) .

This intersection can also be solved graphically. The concept is illustrated in Figure 4.6 for the case of two plants and a dimension of two.

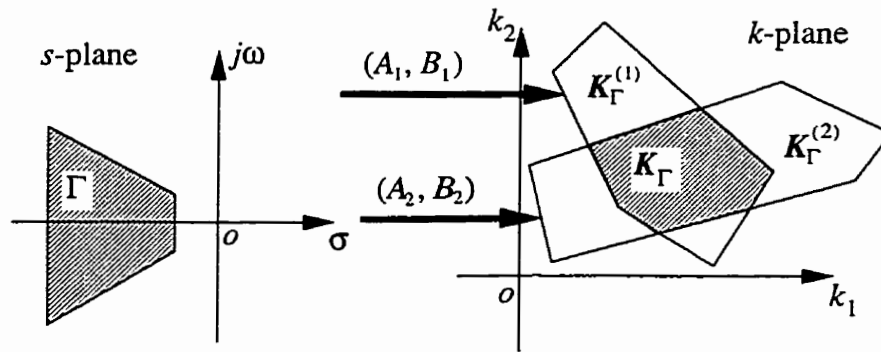


Figure 4.6 Graphical interpretation of simultaneous stabilization based on regional eigenvalue assignment

As illustrated in the preceding section, the design of a reliable controller can be reduced to the simultaneous stabilization problem. Therefore, the above regional eigenvalue assignment technique offers another solution to the reliable control problems. For example, the feedback gain required to stabilize the system against sensor failures can be found in the mapped k -space as shown in Figure 4.7.

The effect of a sensor failure can be multiplicative and additive, which has been discussed in Chapter 2. Multiplicative failures result in reduced sensor gain, and additive failures result in a bias or noise at the output. Multiplicative sensor failures have more effect on the eigenvalue location of the closed-loop system characteristic equation. In the

case of system states being the measured variables, sensor failures can lead to the reduction of the feedback gains.

Assuming that the admissible region for state-feedback gains K_Γ is the triangle ABC , robustness against a sensor failure can be achieved if the projection of $K \in K_\Gamma$ on the subspace for $k_i = 0$ or $k_j = 0$ is still contained in K_Γ . Therefore, for the failure of sensor i (i.e. k_i goes to zero), $DGHI$ is the admissible region, similarly, $JBKEF$ is robust against the failure of sensor j . Finally the intersection $EFML$ is the admissible region for maintaining the system stability against a failure in either sensor i or sensor j .

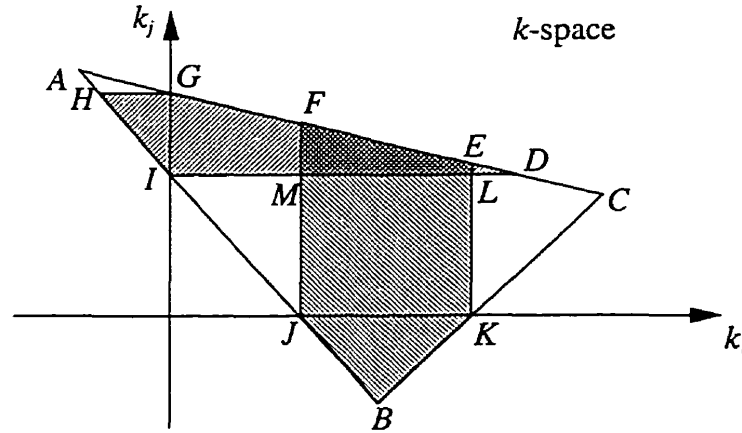


Figure 4.7 An admissible region of the state-feedback gain to guarantee the system stability against sensor failure, [15]

In the case of the non-existence of such an intersection, two choices are given by Ackermann in [15]. One is to rearrange the problem by relaxing the design specifications and to obtain a more relaxed admissible region in the parameter space. The other is to use redundant sensors, for example, a triple sensor redundancy scheme, which has already been applied in practice and has achieved good performance against sensor failures.

So far, previous works on reliable control system design have been briefly introduced. In these works, the design freedom of multivariable systems has been utilized effectively to achieve robustness against system component failures, with different problem formulations and conditions. However, one common drawback is that the concept of redundancy and its importance are still obscure in these works. In Chapter 3, the redundancy in FTCS was investigated in depth and its importance was emphasized therein. In the following section, based on the concept of actuator redundancy defined in Chapter 3, a new passive fault tolerant control design technique against actuator failures is developed. The proposed method possesses an explicit physical insight in each step.

4.3 Passive FTCS Design Against Actuator Failures

4.3.1 Problem formulation

To design a truly reliable control system, one not only has to use high quality system components, but also has to provide enough degree of redundancy in the system in terms of redundant sensors, actuators, and controllers. Generally speaking, hardware redundancy naturally leads to a multiple-input and multiple-output (MIMO) system. It is known that even traditional controller design approaches for MIMO systems is complex and difficult due to the interactions among all system inputs and outputs. Therefore, the design problem of synthesizing a reliable controller for a MIMO system under different fault scenarios becomes even more complicated. Although for a given system, one can always analyze the hardware redundancy based on the condition given in Chapter 3, the problem of how to manage such redundancies and use them to design a reliable controller is still challenging. A good reliable control system design procedure should allow designers to have full access to and utilization of such redundancies.

In this section, only a single output system is considered. Since redundant actuators lead to multiple inputs in the system, the system thus has a MISO representation.

Consider a linear MISO system given as:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t)\end{aligned}\tag{4.40}$$

where $x(t) \in \mathbb{R}^{n \times 1}$, $u(t) \in \mathbb{R}^{m \times 1}$, and $y(t) \in \mathbb{R}^{1 \times 1}$ are the system state vector, the actuator input vector, and the system output, respectively, and the matrices, A, B, C , are of appropriate dimensions. It is assumed that the system satisfies the conditions of Definition 3.2 in Chapter 3, therefore, the system has $(m - 1)$ degrees of actuator redundancy.

As illustrated in Chapter 2, actuator failure can be modeled by relating the actuator output signal, $u_a(t)$, to its input signal, $u(t)$, as:

$$u_a(t) = L_a \cdot u(t) + (I - L_a) \cdot f_a\tag{4.41}$$

where L_a is the failure mode matrix as modelled in EQ(2.7). The constant f_a , in this case, is an offset in the actuator output which is caused by the failure of the actuator. It corresponds to the value at which the actuator is stuck. From the above representation, the system with possible actuator failures can be represented in the state space form by:

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu_a(t) \\ &= Ax(t) + BL_a u(t) + B(I - L_a)f_a \\ y(t) &= Cx(t)\end{aligned}\tag{4.42}$$

In general, because different actuators affect the system from different input locations, the system has non-uniform actuator redundancy, or in other words, rank of the input matrix B is not unity in this case (i.e. $\text{rank}[B] > 1$).

The system in EQ (4.42) can also be represented in the transfer function form as:

$$Y(s) = G_f(s) U(s) + F(s) \quad (4.43)$$

where

$$\begin{aligned} G_f(s) &= G(s) L_a = \frac{N(s) L_a}{d_o(s)} = \frac{1}{d_o(s)} \begin{bmatrix} n_1(s) & n_2(s) & \dots & n_p(s) \end{bmatrix} L_a \\ F(s) &= \frac{N(s) (I - L_a)}{d_o(s) s} f_a \end{aligned} \quad (4.44)$$

where $G(s)$ represents the nominal system, and $G_f(s)$ stands for the system with actuator failures. The n th order polynomial $d_o(s)$ is the characteristic polynomial of the dynamic system, and $N(s)$ is the numerator polynomial vector of the dimension $1 \times m$. $F(s)$ corresponds to the bias caused by the actuator failures.

It should be noted that there are 2^m possible actuator failure modes in total represented by the combination of the elements in L_a . However, we will only consider $2^m - 1$ modes, excluding the case where L_a is a zero matrix (i.e. there should at least be one healthy actuator available in the system). This requirement is essential for the proposed scheme to deal with open-loop unstable systems.

The structure of the overall system is illustrated in Figure 4.8. The overall control system consists of: (i) a dynamic pre-compensator, $P(s)$; (ii) a state-feedback controller, K ; and (iii) a PI controller, $PI(s)$.

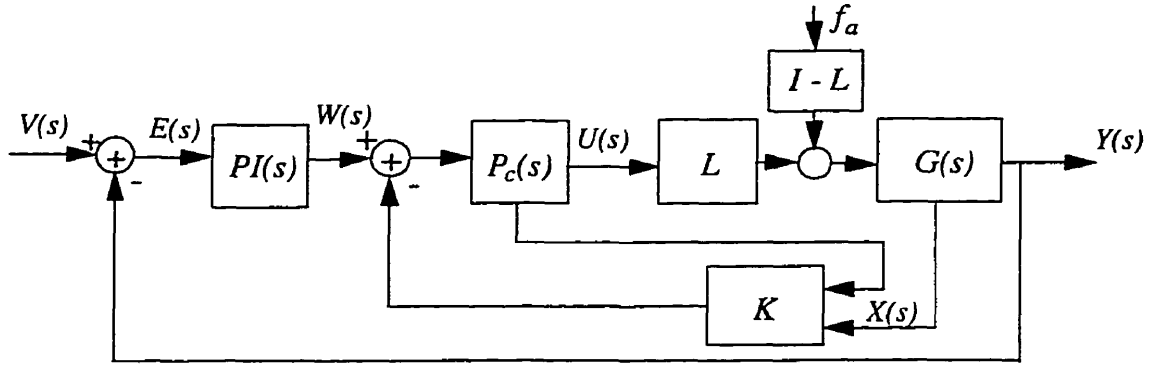


Figure 4.8 The closed-loop system structure of the proposed passive FTCS

There are two main steps involved in the design process:

- (1) Convert the non-uniform actuator redundancy to a uniform one by using a properly chosen dynamic pre-compensator; and
- (2) Select state-feedback as well as *PI* controller gains using the regional eigenvalue assignment technique.

It is important to note that the *PI* regulator is used mainly to eliminate the bias introduced by the malfunctioning actuator (stuck faults) in order to achieve the desired steady-state performance. However, we have to make sure that the good *steady-state* performance is not achieved at the expense of the *transient* performance of the system. Therefore, for a satisfactory performance in both transient and steady-state regions, the *PI* controller and the state feedback controller should be designed simultaneously. In the literature, there have been extensive research efforts on robust servomechanism problem. The resulting controller is robust in the sense that it achieves system tracking ability even in the presence of perturbations of the linear model [16]. However, when there is an actuator failure, the fault induced change is usually large and more drastic. In this case, one has to take use of the actuator redundancy to compensate for such a failure.

4.3.2 Design of the Pre-compensator

For the system given in EQ (4.43), a pre-compensator of the following diagonal matrix form is used:

$$P_c(s) = \frac{1}{d_c(s)} \text{diag}[h_1(s) \ h_2(s) \ \dots \ h_m(s)] = \frac{1}{d_c(s)} H(s) \quad (4.45)$$

where $d_c(s)$ is a Hurwitz polynomial chosen such that every element in $P_c(s)$ is proper.

The choice of the numerator polynomials, $h_i(s)$, depends on the numerator polynomial vector of the nominal system, i.e. $N(s)$. From $N(s) = [n_1(s) \ n_2(s) \ \dots \ n_m(s)]$, the least common polynomials of $n_i(s)/b_i$, $i = 1, 2, \dots, m$, can be obtained, where $b_1, b_2, \dots, b_m$ are the coefficients of the highest power terms in $n_i(s)$, $i = 1, 2, \dots, m$, respectively. Let this least common polynomial be denoted by:

$$n_c(s) = s^r + g_{r-1}s^{r-1} + \dots g_0 \quad (4.46)$$

The elements of the numerator polynomial vector of the pre-compensator, $h_1(s), h_2(s), \dots, h_m(s)$, can then be determined as follows:

$$h_1(s) = \frac{n_c(s)}{n_1(s)/b_1}, h_2(s) = \frac{n_c(s)}{n_2(s)/b_2}, \dots, h_m(s) = \frac{n_c(s)}{n_m(s)/b_m} \quad (4.47)$$

With such a pre-compensator, the augmented system becomes:

$$G_A(s) = G_f(s) P_c(s) = \frac{N(s) L_a H(s)}{d_o(s) d_c(s)} = \frac{N(s) H(s) L_a}{d_o(s) d_c(s)} \quad (4.48)$$

It should be pointed out that because the matrices $H(s)$ and L_a are both diagonal, their positions are interchangeable. From EQ (4.47), one can obtain that:

$$\begin{aligned}
 N(s)H(s) &= \begin{bmatrix} n_1(s) & n_2(s) & \dots & n_p(s) \end{bmatrix} \begin{bmatrix} h_1(s) & 0 & \dots & 0 \\ 0 & h_2(s) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & h_m(s) \end{bmatrix} \\
 &= \begin{bmatrix} b_1 n_c(s) & b_2 n_c(s) & \dots & b_m n_c(s) \end{bmatrix} \\
 &= n_c(s) \begin{bmatrix} b_1 & b_2 & \dots & b_m \end{bmatrix}
 \end{aligned} \tag{4.49}$$

By denoting $\bar{b} = \begin{bmatrix} b_1 & b_2 & \dots & b_m \end{bmatrix} \in \mathbb{R}^{1 \times p}$, the polynomial $N(s)H(s)$ can further be written as:

$$N(s)H(s) = n_c(s) \bar{b} = \left(s^r + g_{r-1}s^{r-1} + \dots + g_0 \right) \bar{b} \tag{4.50}$$

It is worthwhile to point out that EQ (4.50) basically implies that every actuator channel in the compensated system has the same dynamic characteristics, and may only differ by constant gains as specified in the vector $\bar{b}$.

Without any loss of generality, let us assume that the denominator polynomial of the compensated system has the following form:

$$D(s) = d_o(s) d_c(s) = s^q + d_{q-1}s^{q-1} + d_{q-2}s^{q-2} + \dots + d_1s + d_0 \tag{4.51}$$

The order of the compensated system, denoted by q , has now become the sum of the order of the nominal system and that of the pre-compensator.

With an appropriate choice of the state variables, the transfer function matrix in EQ (4.48) can be represented in the following form:

$$\begin{aligned}
\dot{x}_a(t) &= \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -d_0 & -d_1 & -d_2 & \dots & -d_{q-1} \end{bmatrix} x_a(t) + \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \\ b_1 & b_2 & b_3 & \dots & b_m \end{bmatrix} u_a(t) \\
&= A_a x_a(t) + B_a L_a u(t) + B_a (I - L_a) f_a \\
y(t) &= [g_0 \ g_1 \ \dots \ g_{r-1} \ 1 \ 0 \ \dots \ 0] x_a(t) = C_a x_a(t)
\end{aligned} \tag{4.52}$$

From Definition 3.3 in Chapter 3, it is clear that EQ (4.52) represents a system with *uniform* actuator redundancy ($\text{rank}[B] = 1$).

It should be emphasized that the dynamic pre-compensator plays an important role in the overall reliable control system design. The use of the pre-compensator converts the *non-uniform* actuator redundancy to a *uniform* one. More explicitly, it equalizes the dynamic characteristics of different actuator channels by compensating these channels with additional dynamics. By doing so at the first stage of the design, it significantly simplifies the controller gain selection process in the later stage. In practice, the pre-compensator will be implemented as a part of the controller.

From the selection procedure of the pre-compensator, it can be seen that there exists some degree of freedom in choosing the denominator $d_c(s)$. The following guidelines have proved to be useful:

(1) The order of $d_c(s)$ should at least be equal to the highest order of the numerator polynomial of the pre-compensator, $h_i(s)$, for causality. Therefore, the minimum order of the pre-compensator depends entirely on the numerator order of the system model.

(2) $d_c(s)$ should not have any common roots with the numerator polynomial vector of the nominal system, $N(s)$, in order to maintain the controllability of the system.

Furthermore, such freedom in choosing $d_c(s)$ proves to be helpful in the synthesis of the feedback gain in the later stage. In fact, the very concept of employing pre-compensators in reliable control system design is not new. It has been shown by Ackermann in [15] that one of the advantages of using a dynamic pre-compensator is that the solution space of the reliable control system can be enlarged significantly. Consequently, solutions to reliable control system design problems can be found for the system where there were no solutions before.

4.3.3 Design of reliable state feedback and the PI controller

As can be seen from Figure 4.8, in addition to the pre-compensator, the inner loop of the system also consists of a state-feedback controller K , where

$$K = [k_{i,j}], \quad \begin{matrix} i = 1, 2, \dots, m \\ j = 1, 2, \dots, q \end{matrix} \quad (4.53)$$

With the state-feedback, from EQ (4.52), one can obtain that:

$$A_a - B_a L_a K = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -\left(d_0 + \sum_{i=1}^m b_i l_i k_{i1}\right) & -\left(d_1 + \sum_{i=1}^m b_i l_i k_{i2}\right) & -\left(d_2 + \sum_{i=1}^m b_i l_i k_{i3}\right) & \dots & -\left(d_{q-1} + \sum_{i=1}^m b_i l_i k_{iq}\right) \end{bmatrix} \quad (4.54)$$

The inner loop transfer function from $W(s)$ to $Y(s)$ can be expressed as:

$$Y(s) = \frac{n_c(s) \bar{b} L_a}{Q(s)} W(s) + \frac{n_c(s) \bar{b} (I - L_a)}{Q(s) s} f_a \quad (4.55)$$

where the denominator polynomial can be obtained from EQ (4.54) as follows:

$$\begin{aligned} Q(s) &= \text{Det}(sI - (A_a - B_a L_a K)) \\ &= s^q + \left(d_{q-1} + \sum_{i=1}^m b_i l_i k_{iq} \right) s^{q-1} + \dots + \left(d_0 + \sum_{i=1}^m b_i l_i k_{i1} \right) \end{aligned} \quad (4.56)$$

It can be noticed from EQ (4.56) that each column of the matrix K affects only one coefficient in the above characteristic equation. Such a feature is a direct result of the *uniform* redundancy, which makes the synthesis of the controller less complicated.

In the outer loop, a *PI* controller is used to achieve desired steady-state performance in the presence of actuator failures. A more detailed structure of the overall system is shown in Figure 4.9.

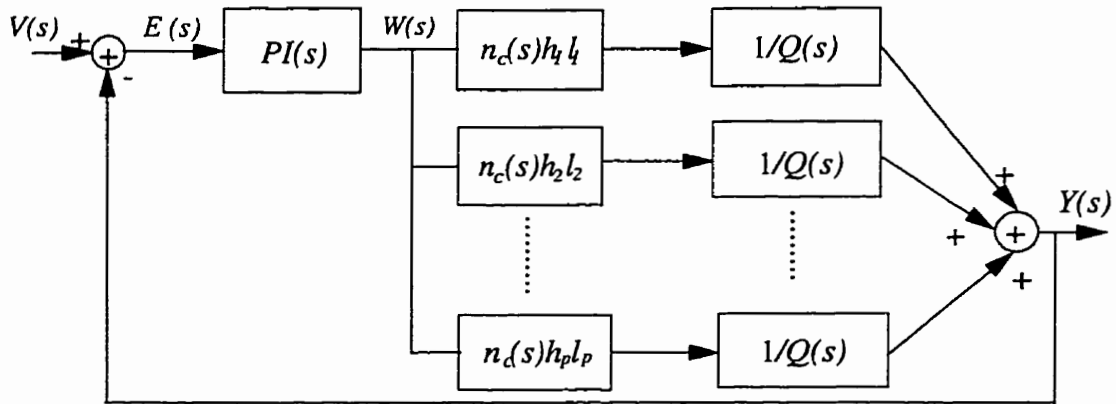


Figure 4.9 The block diagram representation of the passive FTCS

By some simple block diagram manipulation, the transfer function of the closed-loop system can be obtained as:

$$Y(s) = \frac{n_c(s) PI(s) \sum_{i=1}^m b_i l_i}{Q(s) + n_c(s) PI(s) \sum_{i=1}^m b_i l_i} V(s) + D_f(s) \quad (4.57)$$

$$D_f(s) = \frac{n_c(s) \sum_{i=1}^m b_i (1 - l_i) f_a}{sQ(s) + sn_c(s) PI(s) \sum_{i=1}^m b_i l_i} \quad (4.58)$$

where $V(s)$ is the system command input.

Assuming that the PI regulator has the following form:

$$PI(s) = k_p + \frac{k_i}{s} \quad (4.59)$$

where $\{k_p, k_i\}$ are the proportional and the integral gains of the PI regulator.

By substituting EQ (4.59) into EQ (4.58), it is clear that:

$$\begin{aligned} d_f(\infty) &= \lim_{s \rightarrow 0} s \cdot D_f(s) = \lim_{s \rightarrow 0} \frac{s \cdot n_c(s) \sum_{i=1}^m b_i (1 - l_i) f_a}{sQ(s) + sn_c(s) PI(s) \sum_{i=1}^m b_i l_i} \\ &= \lim_{s \rightarrow 0} \frac{s \cdot n_c(s) \sum_{i=1}^m b_i (1 - l_i) f_a}{sQ(s) + s \cdot n_c(s) \cdot k_p \sum_{i=1}^m b_i l_i + n_c(s) \cdot k_i \sum_{i=1}^m b_i l_i} = 0 \end{aligned} \quad (4.60)$$

Therefore, the effect of the actuator failure in the steady-state can be eliminated by the PI controller, provided that the closed-loop system is stable.

The characteristic equation of the closed-loop system EQ (4.57) can further be written in the following form by using EQ (4.59):

$$\begin{aligned} Q_c(s) &= sQ(s) + sk_p n_c(s) \sum_{i=1}^m b_i l_i + k_i n_c(s) \sum_{i=1}^m b_i l_i \\ &= s^{q+1} + d_q s^q + d_{q-1} s^{q-1} + \dots + d_0 \end{aligned} \quad (4.61)$$

It can also be seen clearly that EQ (4.61) allows us to design both the state feedback controller and the *PI* regulator simultaneously to achieve the desired transient and steady-state performance. Hence, the problem of reliable control design becomes synthesizing a feedback gain matrix, K , and a *PI* regulator, such that, for any combination of actuator failure modes, the roots of the characteristic equation in EQ (4.61) remain inside the desired stability region in the s -plane.

Instead of using the Γ -stability region depicted in Figure 4.5, here a degenerated yet effective Γ -stability region is employed, which is shown in Figure 4.10. This region may further degenerate to an open half plane on the left of a straight line at $\sigma = -\sigma_1$. The eigenvalues in this open half plane will guarantee the stability of the closed-loop system with a stability margin, at least σ_1 .

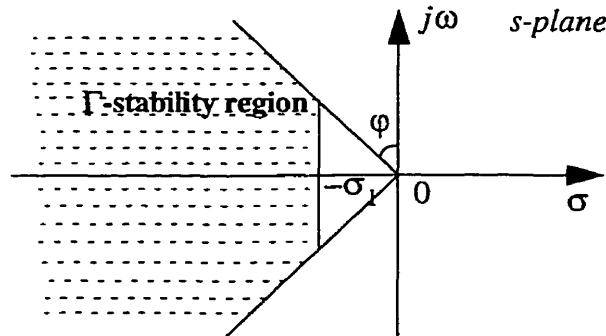


Figure 4.10 The Γ -stability region used in the proposed method

This would have been a standard eigenvalue assignment problem if L_a had always been an identity matrix. However, in our case, there are $2^m - 1$ different combinations of L_a that have to be taken into consideration. Therefore, in this case, we are unable to specify the exact locations for the eigenvalues of the closed-loop system, only a desired region can be specified.

Although there has been extensive research work done on the robust stability of a polynomial subject to parameter perturbations, which are based on Kharitonov's theorem and its various generalizations, [17], unfortunately, they are not suitable for our problem. These works deal mainly with robustness analysis instead of controller synthesis. Although the robust control problem can be clearly defined and well posed from a mathematical point of view, there are no necessary and sufficient conditions for the existence of a robustly stabilizing controller, [15]. Furthermore, the control problem discussed here is even more difficult, since we are dealing with actuator failures which are manifest themselves as large changes in the coefficients of the characteristic polynomial rather than parameter perturbations.

In order to calculate the values of the feedback gain matrix, K , and the PI controller parameters from the coefficients of the characteristic equation EQ (4.61), the first step is to convert the desired stability region in the s -plane into the corresponding interval polynomial in the parametric space, [14][15]. In 1991, Soh et al. proposed a numerical algorithm to evaluate the maximal upper and lower bounds on the coefficients of a given polynomial such that the roots of the interval polynomial are within the specified region in the s -plane, [18]. However, this scheme cannot be used directly for our problem because the obtained bounds are usually too small and conservative to deal with large coefficient changes caused by actuator failures.

Instead of using a single nominal polynomial ($P_0(s)$ in (A.3), see Appendix) to calculate the coefficient intervals, we use a set of nominal polynomials to obtain their

coefficient intervals. A suitable choice of such a polynomial set is the following $(q + 1)$ th order Binomial polynomial with an intermediate parameter σ (the coefficients are varied by changing σ). This nominal polynomial set is named as the reference polynomial set.

$$\Psi(s, \sigma) = (s + \sigma)^{q+1} = s^{q+1} + \alpha_q(\sigma)s^q + \alpha_{q-1}(\sigma)s^{q-1} + \dots + \alpha_0(\sigma) \quad \sigma > 0 \quad (4.62)$$

For every chosen σ , the coefficient intervals of the above polynomial can be determined. This will generate an interval polynomial set whose coefficient bounds are also functions of the intermediate parameter σ :

$$\Phi(s, \sigma) = s^{q+1} + [\underline{\alpha}_q(\sigma), \bar{\alpha}_q(\sigma)]s^q + [\underline{\alpha}_{q-1}(\sigma), \bar{\alpha}_{q-1}(\sigma)]s^{q-1} + \dots + [\underline{\alpha}_0(\sigma), \bar{\alpha}_0(\sigma)] \quad (4.63)$$

From the above interval polynomial set, a so-called $\mathcal{Q}$ - box set can be defined as:

$$\mathcal{Q} = \{ \Omega(\sigma) \mid \alpha_i(\sigma) \in [\underline{\alpha}_i(\sigma), \bar{\alpha}_i(\sigma)], i = 0, 1, \dots, q \} \quad (4.64)$$

where $\underline{\alpha}_i(\sigma) = \alpha_i(\sigma) - \tau_i \varepsilon$, $\bar{\alpha}_i(\sigma) = \alpha_i(\sigma) + \mu_i \varepsilon$. $\varepsilon > 0$ is the size of the perturbation used in the bound computation, and τ_i, μ_i are the corresponding weights on each perturbation ((A.1), see Appendix). It is clear that this $\mathcal{Q}$ - box set represents a set of stable interval polynomials. With an appropriate choice of the weights, most of the practical stability regions, such as the Γ -stability region, can be dealt with. By using the $\mathcal{Q}$ - box set the admissible coefficient space for guaranteeing the stability is enlarged significantly. When calculating the coefficient bounds, they are no longer restricted to only one nominal polynomial. Instead, a number of overlapped coefficient bounds can be obtained by varying σ continuously as shown in EQ (4.64).

Even though the above reference polynomial set in EQ (4.62) looks simple, it has several desirable properties: (i) there is only a single intermediate parameter needs to be adjusted, which makes the coefficient bounds calculation straightforward; and (ii) the stability margin of the system associated with this polynomial set is simply the parameter

imaginary axis, the intervals in the parametric space tend to increase as well, i.e. the size of the Q -box increases. Therefore, by moving the intermediate parameter σ continuously, an enveloped region containing a set of overlapped squares, will be obtained, which is shown as the shaded region in the parametric space. The importance of this region lies in the fact that, for any polynomial whose coefficients are in this region, its roots will be in the corresponding desired region on the s -plane.

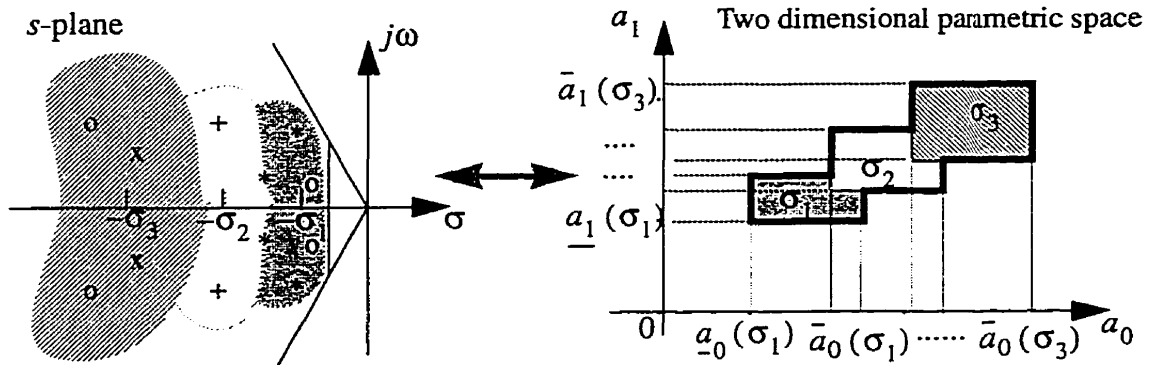


Figure 4.11 Geometric interpretation in the parametric space

It should be pointed out that the solution of the reliable state-feedback controller K satisfying the inequalities EQ (4.65) is not unique. Therefore, depending on different applications, additional design requirements can be employed to select a specific K in the feasible solution space.

4.3.4 Design examples

1. A reliable bank angle control system

The model used in this example represents a bank-angle control system for a jet transport aircraft, flying at the speed of 0.8 Mach and an altitude of 40,000 ft. There are two manipulated variables: the aileron, and the rudder. The variable being controlled is the

bank-angle of the aircraft. It is desirable that the bank-angle be kept at a desired value even in the presence of failures in either the aileron or the rudder.

In a typical flight control system, pilots or AFCS (Automatic Flight Control Systems) mainly use the aileron to control the bank-angle of the roll motion. However, because there exists dynamic coupling between the yaw and the roll motions, it is also possible to control the bank-angle using the rudder. In this respect, the rudder can be considered a redundant control actuator. It can then be used during an emergency when the aileron control channel malfunctions. This example illustrates how to design a reliable control system with such actuator redundancies so that the stability of the bank-angle control system as well as the steady-state tracking performance can be maintained in the presence of actuator failures.

The model of the nominal system is given as follows:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} -0.0558 & -0.9968 & 0.0802 & 0.0415 \\ 0.5980 & -0.1150 & -0.0318 & 0.0 \\ -3.0500 & 0.3880 & -0.4650 & 0.0 \\ 0.0 & 0.0805 & 1.0000 & 0.0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} 0.0729 & 0.0001 \\ -4.7500 & 1.2300 \\ 1.5300 & 10.6300 \\ 0.0 & 0.0 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad (4.66)$$

$$y = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

where the states x_i , $i = 1, 2, 3, 4$ are the sideslip angle (rad), the yaw rate (rad/sec), the roll rate (rad/sec), and the bank angle (rad), respectively. The inputs u_1 and u_2 are the rudder and the aileron, respectively. The output y is the bank angle. From the structure of the input matrix, it can be seen that the actuator redundancy belongs to the *non-uniform*

class. Physically, this means that the aileron and the rudder affect the bank angle of the aircraft differently.

The transfer function matrix for this system can be obtained as follows:

$$G(s) = \frac{\begin{bmatrix} 1.1476s^2 - 2.0036s - 13.7264 & 10.7290s^2 + 2.3169s + 10.2370 \end{bmatrix}}{s^4 + 0.6358s^3 + 0.9389s^2 + 0.5116s + 0.0037} \quad (4.67)$$

The eigenvalues of the open-loop system are:

$$\Lambda = \begin{cases} -0.0329 \pm j0.9467 \\ -0.5627 \\ -0.0073 \end{cases} \quad (4.68)$$

Based on the design procedure for the pre-compensator presented in Section 4.3.2, a dynamic pre-compensator is chosen as follows:

$$P(s) = \text{diag} \left[\frac{s^2 + 0.216s + 0.9541}{s^2 + 1.1s + 0.3} \quad \frac{s^2 - 1.7459s - 11.9611}{s^2 + 1.1s + 0.3} \right] \quad (4.69)$$

It should be noted that the denominator of the pre-compensator is chosen according to the guidelines specified in Section 4.3.2.

With such a pre-compensator, the augmented system can be represented as follows:

$$\begin{aligned} \dot{x}_a(t) &= A_a x_a(t) + B_a \begin{bmatrix} l_1 & 0 \\ 0 & l_2 \end{bmatrix} u(t) + B_a \begin{bmatrix} 1 - l_1 & 0 \\ 0 & 1 - l_2 \end{bmatrix} f_a \\ y(t) &= C_a x_a(t) \end{aligned} \quad (4.70)$$

where f_a is the unknown actuator offset caused by the failure, and the numerical values for the system matrices are given below:

$$A_a = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -0.0011 & -0.1576 & -0.8481 & -1.7351 & -1.9383 & -1.7358 \end{bmatrix} \quad (4.71)$$

The input matrix is:

$$B_a = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1.1476 \\ 0 & 0 & 0 & 0 & 0 & 10.7290 \end{bmatrix}^T \quad (4.72)$$

and the output matrix is:

$$C_a = [-11.4123 \quad -4.2494 \quad -11.3841 \quad -1.5299 \quad 1 \quad 0] \quad (4.73)$$

Clearly, EQ (4.72) indicates that the redundancy of the system has been converted into a *uniform* type through the use of the pre-compensator of EQ (4.69).

From the design procedure illustrated in Section 4.3.3, the following state-feedback gain matrix as well as the *PI* controller parameters can be obtained. In the design of the controller, the intermediate parameter σ is varied from -0.1 to -4.5 when computing the coefficient interval set in EQ (4.64), and the desired pole assignment region is the stripe between these two values in the left-half s -plane.

$$K = \begin{bmatrix} 4.9197 & 21.6529 & 34.6934 & 30.2875 & 15.9917 & 3.0230 \\ 2.0517 & 6.4617 & 10.8289 & 10.1678 & 4.1151 & 0.7277 \end{bmatrix} \quad (4.74)$$

$$PI(s) = \frac{-0.0639s - 0.0448}{s} \quad (4.75)$$

In addition, the above K is obtained by minimizing the real part of the largest eigenvalue of the closed-loop system under all actuator failure cases.

The eigenvalues of the closed-loop system under all three modes of operation are illustrated as follows:

(A) During normal operation:

$$\Lambda = \begin{cases} -4.0120 \\ -3.9878 \\ -3.0001 \\ -1.0782 \\ -0.3468 \\ -0.2937 \pm j0.5001 \end{cases} \quad (4.76)$$

where the first three values correspond to the eigenvalues of the pre-compensator.

(B) Under the aileron failure:

$$\Lambda = \begin{cases} -0.2063 \\ -0.2351 \\ -0.8055 \\ -0.6115 \pm j1.0587 \\ -1.3675 \pm j2.8579 \end{cases} \quad (4.77)$$

(C) Under the rudder failure:

$$\Lambda = \begin{cases} -0.3405 \\ -0.9712 \\ -2.9570 \\ -0.2087 \pm j0.5478 \\ -2.4285 \pm j3.2267 \end{cases} \quad (4.78)$$

These eigenvalues clearly indicate that the stability of the system is well maintained in all three operational modes. The simulation has been performed. With the system configuration as shown in Figure 4.8, the tracking ability of the system will be maintained

with the help of the *PI* controller in the outer loop. The step responses of the system under all three modes of operation are shown in Figure 4.12.

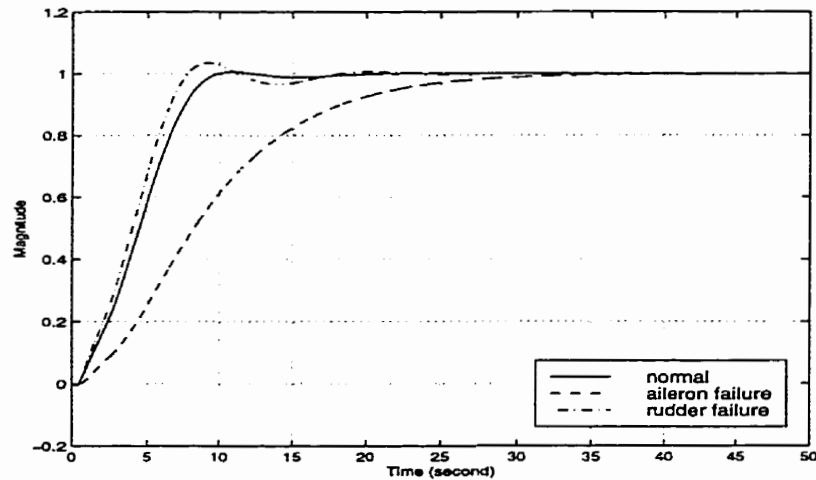


Figure 4.12 Step response of the closed-loop system in three operation modes

From Figure 4.12, one can observe that when an aileron failure occurs, the system becomes much more sluggish. This is because the aileron is the primary actuator for the bank-angle control. On the other hand, if failure occurs in the rudder, the system experiences slightly more overshoot because during normal operation, the rudder provides additional damping to the closed-loop system. We should emphasize that the steady-state performance of the system is maintained under all three conditions.

The step response of the normal system is shown in Figure 4.13 (a), together with the control signals to the aileron and rudder shown in Figure 4.13 (b). In this figure, an input command consists of two step inputs, one occurs at $t = 1 \text{ sec.}$, the other at $t = 40 \text{ sec.}$

It is also interesting to examine how failures in the aileron or the rudder affect the bank-angle control. These two situations are shown in Figure 4.14 and Figure 4.15,

with the same system input as in Figure 4.13. The only difference is that an actuator (aileron or rudder) is assumed to fail at $t = 30\text{sec.}$ before the second step input command is issued.

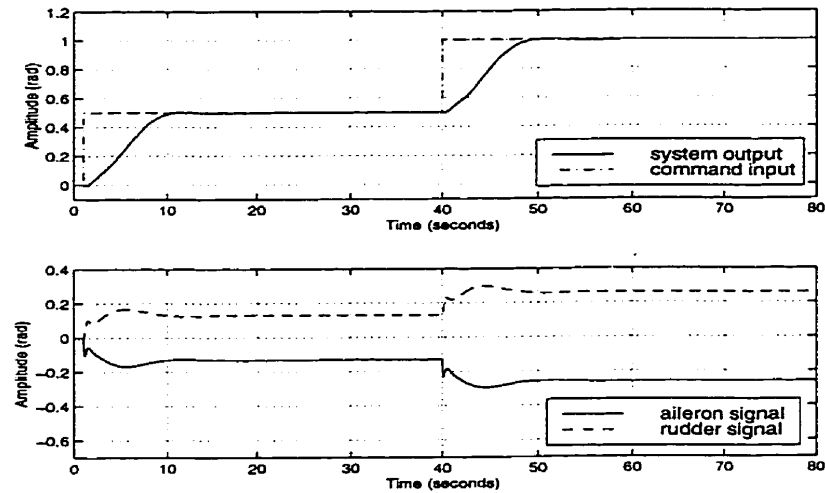


Figure 4.13 Normal operation: (a) System response; (b) Control signals from the aileron and the rudder

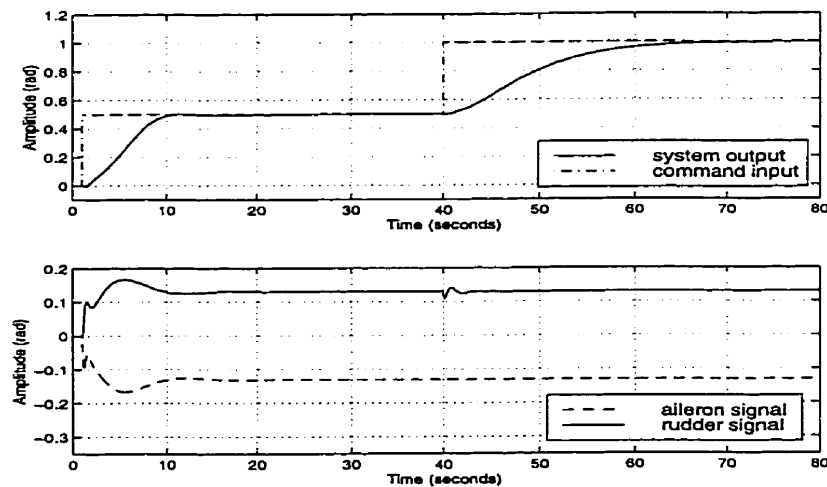


Figure 4.14 Aileron failure: (a) System response; (b) Control signals from the aileron and the rudder

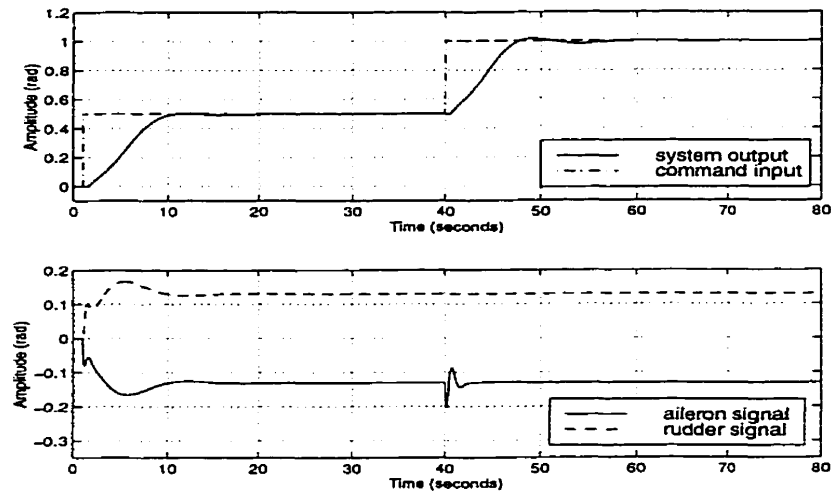


Figure 4.15 Rudder failure: (a) System response; (b) Control signals from the aileron and the rudder

As illustrated in Figure 4.14 and Figure 4.15, when the actuator failure occurs at $t=30$ sec., because the failure results in an offset in the actuator output signal (i.e. the failed actuator is stuck at certain position), it does not affect the system until the input command changes. This can be seen clearly by comparing the three system responses in the three operation modes after $t=40$ sec. Compared to the normal system response in Figure 4.13(a), the response of the system with the aileron failure in Figure 4.14(a) becomes much slower, while the response of the system with the rudder failure in Figure 4.15(a) becomes less damped.

To better understand how the reliable controller achieves the fault tolerance, and the intricate relationships between the aileron and the rudder in the presence of failures, we have depicted the control signals from the rudder channel as well as from the aileron channel in all three operational modes in Figure 4.13(b), Figure 4.14(b) and Figure 4.15(b). These figures clearly show that these two actuators cooperate to achieve the appropriate control and compensate for each other. When one actuator fails, it remains at a certain fixed position, and the other actuator change its control effort immediately to com-

pensate for the failed actuator. This kind of load-sharing is carried out internally and automatically with the proposed design scheme.

2. Reliable dual-actuator ball-beam system

Consider the dual-actuator system as shown in Figure 4.16, The system has two driving motors, one at each end. We can consider one of the two motors as redundant. The function of the two motors is to move the beam at the two ends up and down to control the position of the ball. The type of redundancy illustrated in this system is the actuator redundancy. We will show that it is the existence of such redundancy that makes it possible to design a FTCS against failures in either motor.

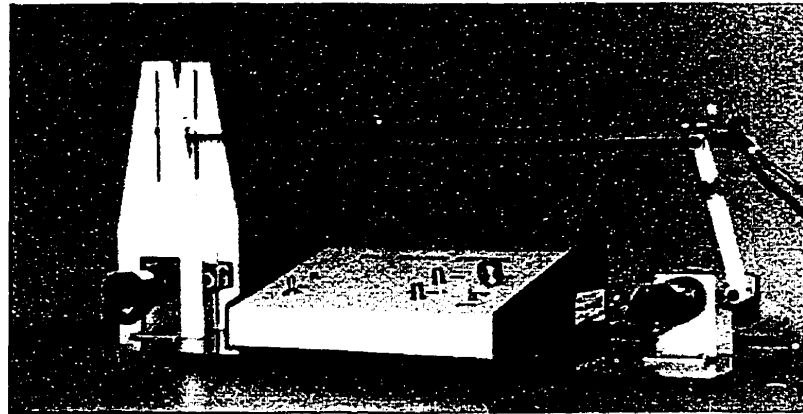


Figure 4.16 Dual-actuator ball-beam system

The kinematic diagram of the system is sketched in Figure 4.17.

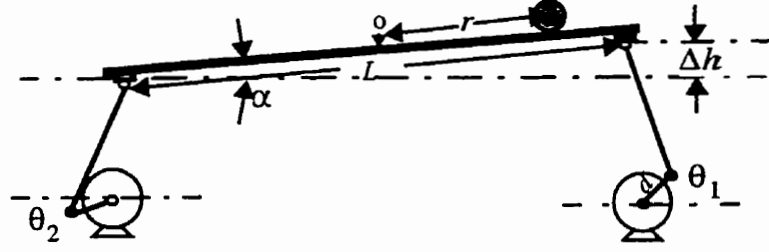


Figure 4.17 Kinematic relationship of the ball-beam system

The physical parameters of the system and their values are as follows:

- L : the beam length (0.5 m)
- r : radius of the ball (0.016 m)
- m : mass of the ball (0.2 kg)
- d : lever offset (0.04 m)
- g : gravitational acceleration (9.807 m/s^2)
- J : moment of inertia of the ball ($\text{Nm s}^2/\text{rad}$)
- η : ball position from the center of the beam (m)
- α : angle of the beam (rad)
- θ_i : gear angle of the i th servo motor (rad).

From the kinematic relationship, a Lagrangian equation can be obtained:

$$\left(\frac{J}{r^2} + m \right) \ddot{\eta}(t) + mg \sin \alpha = 0 \quad (4.79)$$

In the above, the moment of inertia is calculated using the following formula:

$$J = \frac{2}{5} (m \cdot r^2) \quad (4.80)$$

With the assumption that the beam is long enough with respect to Δh , (i.e. α is very small, and $\sin \alpha \approx \alpha$), EQ (4.79) can further be simplified as:

$$\left(\frac{J}{r^2} + m\right)\ddot{\eta}(t) + mg\alpha(t) = 0 \quad (4.81)$$

Furthermore,

$$\Delta h(t) = L \sin[\alpha(t)] \approx L\alpha(t) = d \sin[\theta_1(t)] - d \sin[\theta_2(t)] \quad (4.82)$$

Hence, the system with small perturbations can be expressed as:

$$\alpha(t) = \frac{d}{L} \{ \sin[\theta_1(t)] - \sin[\theta_2(t)] \} \approx \frac{d}{L} [\theta_1(t) - \theta_2(t)] \quad (4.83)$$

where $\theta_1(t)$ and $\theta_2(t)$ are the angular positions of the two driving motors.

Substituting the above equation into EQ (4.81), the following simple linear relationship can be obtained:

$$L\left(\frac{J}{r^2} + m\right)\ddot{\eta}(t) = -mgd[\theta_1(t) - \theta_2(t)] \quad (4.84)$$

Clearly, the system has two independently manipulated variables, $\theta_1(t)$ and $\theta_2(t)$.

The above model can be written in a state-space representation as:

$$\dot{x}(t) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 & 0 \\ \frac{-mgdr^2}{L(J+mr^2)} & \frac{mgdr^2}{L(J+mr^2)} \end{bmatrix} \begin{bmatrix} \theta_1(t) \\ \theta_2(t) \end{bmatrix} \quad (4.85)$$

where the state vector is defined as: $x(t) = [x_1(t) \ x_2(t)]^T = [\eta(t) \ \dot{\eta}(t)]^T$.

Since the motor dynamics are much faster than that of the system, in the subsequent analysis we will ignore the motor dynamics and assume that the motor angular positions are proportional to the applied voltage:

$$\theta_i(t) = K_i u_i(t) \quad i = 1, 2 \quad (4.86)$$

where K_i is the proportional gain of the i th motor.

Combining EQs (4.85) & (4.86), one can obtain the following dynamic relationships between the applied motor voltages, the system inputs, and the ball position as the system output:

$$\begin{aligned} \dot{x}(t) &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 & 0 \\ \frac{-mgdr^2 K_1}{L(J+mr^2)} & \frac{mgdr^2 K_2}{L(J+mr^2)} \end{bmatrix} \begin{bmatrix} u_1(t) \\ u_2(t) \end{bmatrix} \\ y(t) &= \begin{bmatrix} 1 & 0 \end{bmatrix} x(t) \end{aligned} \quad (4.87)$$

This system has two inputs and one output. From the redundancy definition in Chapter 3, it becomes clear that this system has one degree of *uniform* actuator redundancy. This redundant control input can be utilized to improve the fault tolerance capability of the system against possible failure of the driving motors. It should be noted that the precompensator is not needed in this case because the system is already in the uniform redundancy form. In the actual controller implementation, the ball position is obtained by measuring the resistance of the beam, and the ball speed signal is estimated using a numerical differentiator.

The objective of the FTCS design is to synthesize a state-feedback and a *PID* controller which can maintain the desired system performance (stability and accuracy) not only when both motors are in good working condition, but also when one of the motors fails.

Based on the previous analysis, the structure of the closed-loop system can be illustrated in Figure 4.18. There are two control loops in the system. A state-feedback control is used in the inner loop, and a *PID* controller is employed in the outer loop for maintaining the tracking ability. It should be mentioned that in order to guarantee stability in the normal and actuator failure modes of operations, the state-feedback and the *PID* controllers should be considered jointly in the design.

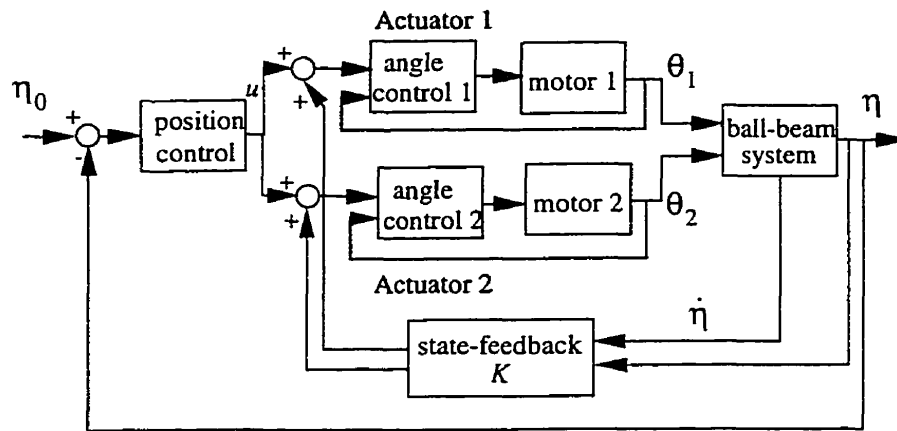


Figure 4.18 The structure of ball-beam balance control system

To synthesize a reliable ball-beam balance control system, the following design objectives need to be satisfied:

1. *High priority objectives*: maintain the closed-loop system stability and achieve a zero steady-state position error.
2. *Low priority objectives*: limit the maximum overshoot/undershoot less than 10% and limit the settling time less than 10 sec.

When both motors operate normally, the high priority objectives and the low priority objectives should be achieved. In other words, the system should be able to balance the ball at any desired location on the beam quickly and in a stable manner. However,

if one of the motors has failed, using the reliable control, the high priority objectives need to be achieved with the possible compromise of the lower priority objectives.

By substituting the values for all the physical system parameters in EQ (4.87), and letting $K_1 = K_2 = 1.0$, the system model becomes:

$$\begin{aligned}\dot{x}(t) &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 & 0 \\ -0.56 & 0.56 \end{bmatrix} \begin{bmatrix} u_1(t) \\ u_2(t) \end{bmatrix} \\ y(t) &= \begin{bmatrix} 1 & 0 \end{bmatrix} x(t)\end{aligned}\quad (4.88)$$

From EQ (4.88), it can be seen that the state-space representation of the system is in the controllability companion canonical form, and the system has one degree of uniform actuator redundancy. By using the design technique presented in Section 4.3, the following state-feedback gain matrix is synthesized:

$$K = \begin{bmatrix} -0.2865 & -0.5901 \\ 0.2865 & 0.5901 \end{bmatrix} \quad (4.89)$$

In addition, the parameters of the PID controller is chosen as:

$$K_P = 2.2 \quad K_I = 1.3 \quad K_D = 3.5 \quad (4.90)$$

With the above chosen state-feedback and PID controller gains, the eigenvalues of the closed-loop system can be calculated as follows for three motor conditions:

$$\begin{aligned}\text{normal: } \lambda_0 &= \{-3.9721, -0.3044 + j0.5233, -0.3044 - j0.5233\} \\ \text{motor 1 failed: } \lambda_1 &= \{-3.6393, 0.3016 + j0.5538, -0.3016 - j0.5538\} \\ \text{motor 2 failed: } \lambda_2 &= \{-3.6393, 0.3016 + j0.5538, -0.3016 - j0.5538\}\end{aligned}\quad (4.91)$$

It is clear that the closed-loop system is stable for all three conditions. However, when one of the motors fails, the system eigenvalues move close to the edge of the Γ -stability region, as shown in Figure 4.10.

To evaluate the performance of the FTCS design, step response tests have been carried out on the system under the following operational modes: (1) both motors are in operation; and (2) only one motor is operational. The experimental results are illustrated in Figure 4.19 & Figure 4.20, respectively. In both cases, the control command is to move the ball 10 cm off the center of the beam.

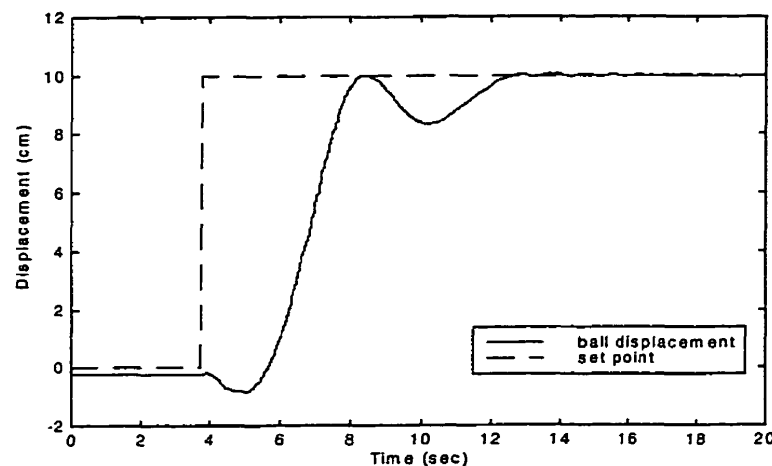


Figure 4.19 Step response of the system under two motor operation

Examining the system responses, it is interesting to note that, when both motors are operational, the system tends to have smaller overshoot/undershoot (less than 19%) and shorter settling time (10 sec.). However, the interaction between the two motors produces a non-minimum phase characteristics which lead to a small undershoot in the initial part of the response. In contrast, single motor results in a larger overshoot (37%), less damping, and longer settling time (14 sec.). Nevertheless, the closed-loop system is still stable.

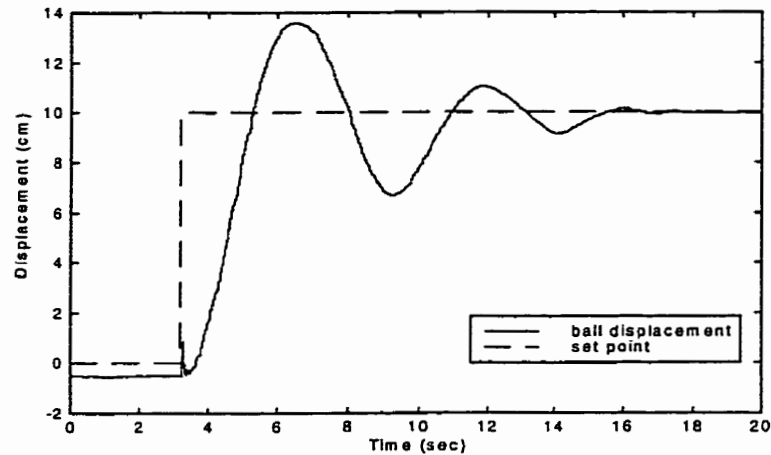


Figure 4.20 Step response of the system under single motor operation

The above feature is common among most fault tolerant control systems, i.e. in the presence of faults, one would expect that there is a limited amount of performance degradation, but the most important properties of the system, such as stability, are maintained.

In order to examine the transient induced by the actuator failure during the operation, we have simulated an actuator fault at $t=4$ sec by disabling one of the motors before the system reaches the steady-state. The result is shown in Figure 4.21. It can be observed that when one motor fails, the other motor can still achieve the final control objective. Of course, the amount of fault-induced transient will depend on the time and the state of the system when the fault occurs. In this case, the fault induced transient lasts about 10 sec.

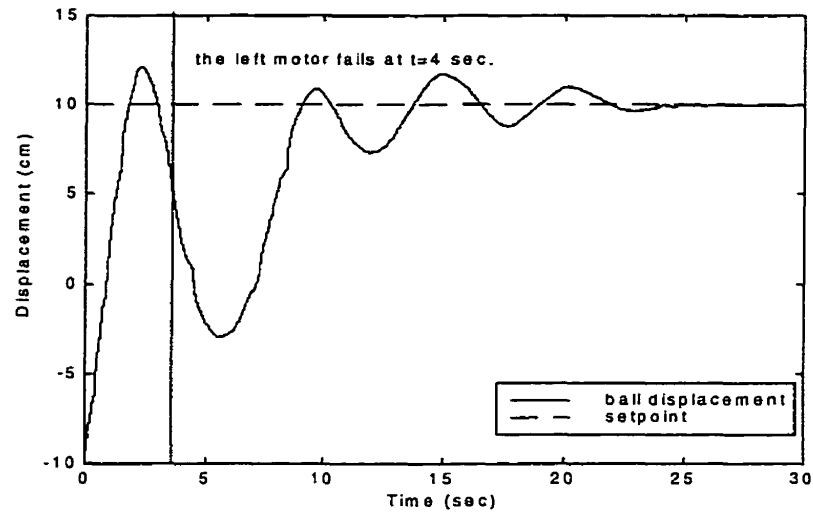


Figure 4.21 Fault-induced transients during the operation

The experimental results have clearly demonstrated the effectiveness of the FTCS design against actuator failures. If the controller is designed without taking into consideration the actuator failures, the system may still operate satisfactorily when both actuators are in good working condition, but can fail catastrophically whenever one of the actuators is out of service. This situation is illustrated in Figure 4.22 where the system initially operates normally with the two actuators, but cannot even maintain the closed-loop stability when one of the motors fails.

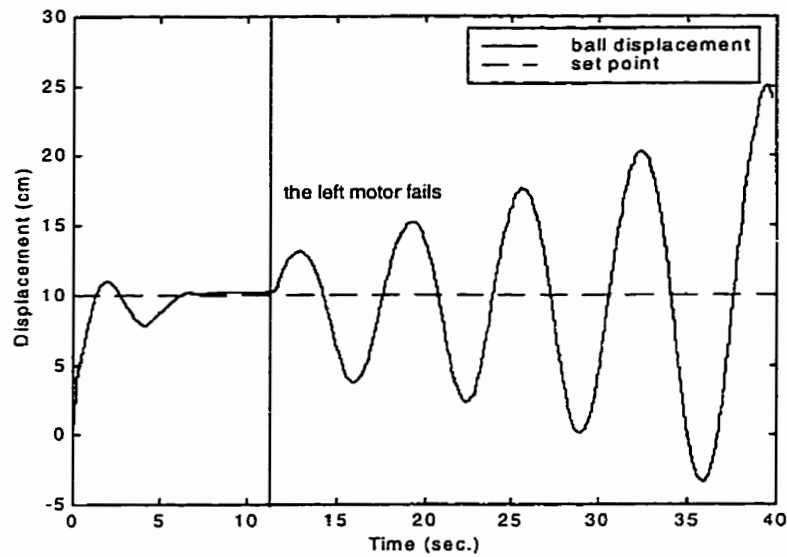


Figure 4.22 Unstable system response under single motor operation using conventional control

4.4 Passive FTCS Design Against Sensor Failures

4.4.1 Problem formulation

Generally speaking, the output sensor plays a very important role in the control system. Usually, sensor failure can pose a very serious problem. For this reason, redundant sensors are often used in systems with high reliability requirements. In fact, triple or quadruple sensor redundancy followed by a voting scheme is a very common technique used in practice. The voting scheme is used to distinguish the normal sensor reading from the abnormal ones and a switching device is used to feed back the proper signal [18] [19]. Such scheme is usually effective in increasing the reliability against sensor failures. However, in some cases, due to the sensor size, the extra cost and the increased complexity of the entire control system, such a scheme may not be practical.

In this section, a reliable control system design scheme against sensor faults is proposed. In addition to the system output sensor, redundant dissimilar sensors are used to measure the other system variables which are accessible. Then additional information on system output can be obtained through an estimation algorithm based on the redundant measurements. Such redundant output signals are extremely important, especially when the output sensor fails. There is no switching action in the proposed control strategy since both the output sensor and the redundant dissimilar sensors are used during the entire system operation. When properly selected, the redundant sensors can have smaller size, lower cost and higher reliability in comparison to the primary output sensor. The proposed control scheme has been implemented on a lab-scale DC motor drive system.

Consider a linear time-invariant SISO system with the input u and the output y , with a reliable control system structure with redundant sensors as given in Figure 4.23. In addition to the primary output sensor (sensor 1), another sensor (sensor 2) is also used to measure a properly chosen intermediate state variable, y_1 . From y_1 , the system output can be estimated and used as the feedback signal to the controller.

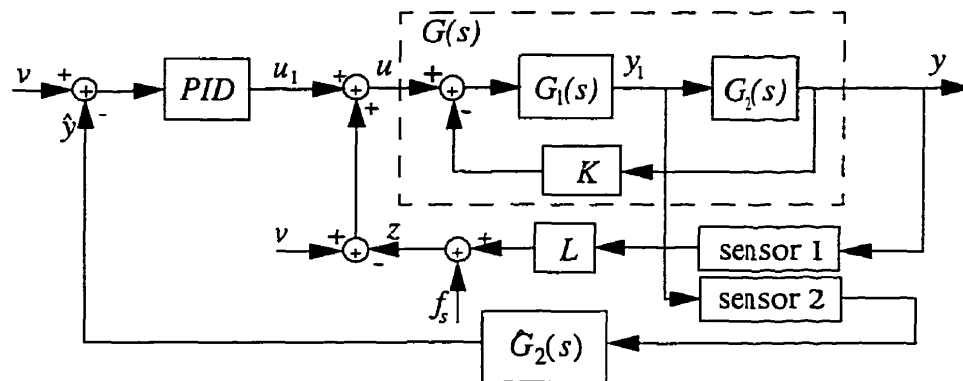


Figure 4.23 The illustrative diagram of the passive control system structure against sensor faults

From Figure 4.23, the system transfer function $G(s)$ is calculated as follows:

$$G(s) = \frac{G_1(s) G_2(s)}{1 + K \cdot G_1(s) \cdot G_2(s)} \quad (4.92)$$

and

$$Y_1(s) = \frac{G_1(s)}{1 + K \cdot G_1(s) \cdot G_2(s)} \cdot U(s) \quad (4.93)$$

$$Y(s) = G_2(s) Y_1(s) \quad (4.94)$$

According to the sensor fault modelling in Chapter 2, the measured system output z with the possible sensor failure is obtained as:

$$Z(s) = L_s \cdot M_1 \cdot Y(s) + (1 - L_s) \cdot f_s \quad (4.95)$$

where M_1 represents the gain of sensor 1, and $f_s(s) = d_f/s$ is the sensor reading deviation due to failure, which, in time domain, is a constant term d_f .

$\hat{G}_2(s)$ is the model of the system dynamics $G_2(s)$. Through $\hat{G}_2(s)$, the system output can be estimated using the intermediate state y_1 , i.e.

$$\hat{Y}(s) = M_2 \cdot \hat{G}_2(s) Y_1(s) \quad (4.96)$$

where $\hat{Y}(s)$ is the estimated system output signal, and M_2 represents the gain of sensor 2.

By assuming $M_1 = 1$ and $M_2 = 1$, EQ (4.95) and EQ (4.96) can be written as:

$$\begin{aligned} Z(s) &= L_s \cdot Y(s) + (1 - L_s) \cdot f_s \\ \hat{Y}(s) &= \hat{G}_2(s) Y_1(s) \end{aligned} \quad (4.97)$$

Given such a system structure, the problem of reliable control is to design the controller such that, under both normal and sensor failure conditions, the closed-loop system stability and a certain performance level can be maintained. It should be mentioned

that in the servo system, the tracking ability of the control system can be achieved by using a *PID* controller.

4.4.2 Design of the control system

From Figure 4.23, by a simple block diagram manipulation, the transfer function of the closed-loop system can be obtained:

$$\begin{aligned}
 Y(s) &= \frac{(G_{pid}(s) + 1) G_1(s) G_2(s)}{1 + G_1(s) \hat{G}_2(s) G_{pid}(s) + (K + L_s) G_1(s) G_2(s)} \cdot V(s) \\
 &\quad + \frac{G_1(s) G_2(s)}{1 + G_1(s) \hat{G}_2(s) G_{pid}(s) + (K + L) G_1(s) G_2(s)} f_s(s) \\
 &= G_c(s) V(s) + D_f(s)
 \end{aligned} \tag{4.98}$$

where $G_{pid}(s) = k_p + \frac{k_i}{s} + k_d s$.

From EQ (4.98), one can further obtain that:

$$\begin{aligned}
 G_c(s) &= \frac{\{k_d s^2 + (k_p + 1)s + k_i\} G_1(s) G_2(s)}{k_d G_1(s) \hat{G}_2(s) s^2 + [k_p G_1(s) \hat{G}_2(s) + (K + L_s) G_1(s) G_2(s) + 1] s + k_i G_1(s) \hat{G}_2(s)} \\
 D_f(s) &= \frac{G_1(s) G_2(s)}{k_d G_1(s) \hat{G}_2(s) s^2 + [k_p G_1(s) \hat{G}_2(s) + (K + L) G_1(s) G_2(s) + 1] s + k_i G_1(s) \hat{G}_2(s)} \times \frac{d_f}{s}
 \end{aligned} \tag{4.100}$$

Therefore, in the steady-state:

$$K_\infty = G_c(s) \big|_{s \rightarrow 0} = \frac{G_2(s) \big|_{s \rightarrow 0}}{\hat{G}_2(s) \big|_{s \rightarrow 0}} \tag{4.101}$$

and

$$D_{f,\infty} = \lim_{s \rightarrow 0} s \cdot \frac{d_f}{s} \cdot \frac{G_1(s) G_2(s) \cdot s}{k_d G_1(s) \hat{G}_2(s) s^2 + (k_p G_1(s) \hat{G}_2(s) + (K + L_s) G_1(s) G_2(s) + 1) s + k_i G_1(s) \hat{G}_2(s)} \quad (4.102)$$

$$= 0$$

where K_∞ is the system DC-gain. One can see clearly that the sensor failure does not affect the steady-state of the system response at all. By assuming that $\hat{G}_2(s) = G_2(s)$. The DC-gain can be maintained at unity independent of L_s . From EQ (4.102), the sensor bias has also been eliminated by the *PID* controller. Therefore, using the above control system structure can indeed guarantee the system steady-state performance in the presence of the output sensor failure. However, the sensor failure can actually affect the system transient performance, and even the system stability. Hence, the controller needs to be carefully designed in order for the system to retain its stability.

By writing $G_c(s)$ in EQ (4.99) as:

$$G_c(s) = \frac{n(s)}{d(s)} \quad (4.103)$$

The characteristic equation of the closed-loop system can then be written as:

$$d(s) = s^q + \alpha_1 s^{q-1} + \alpha_2 s^{q-2} + \dots + \alpha_q \quad (4.104)$$

where q is the order of the closed-loop system, and α_i , $i = 1, \dots, q$ are the coefficients of the closed-loop system characteristic equation, and

$$\alpha_i = \alpha_i(\theta, \hat{\theta}_2, k_p, k_i, k_d, L_s) \quad i = 1, 2, \dots, q \quad (4.105)$$

where θ is a vector containing the coefficients of the denominator polynomial of the transfer function $G(s)$, and similarly $\hat{\theta}_2$ is that of $\hat{G}_2(s)$.

Under normal system operation and output sensor failure operation, one can have the following two different closed-loop characteristic equations:

$$\begin{aligned}\alpha_{i,normal} &= \alpha_i(a, \hat{a}_2, k_p, k_i, k_d, 1) \\ \alpha_{i,failure} &= \alpha_i(a, \hat{a}_2, k_p, k_i, k_d, 0)\end{aligned}\quad i = 1, 2, \dots, q \quad (4.106)$$

Based on the above parameters, one has to choose k_p , k_i , k_d to stabilize the closed-loop system under both normal and sensor failure conditions. The robust eigenvalue assignment technique that has been discussed in the preceding section can also be used here to determine the controller parameters. Therefore, with the proposed system structure and by properly designing the controller parameters, the closed-loop system stability and tracking ability in the normal and the output sensor failure cases can be guaranteed.

An assumption of the proposed scheme is that the system dynamic model is known exactly. However, the modelling error always exists in practice. In this case, the effect of the modelling error can be examined through sensitivity and robustness analysis, [20] [21].

4.4.3 Reliable DC drive system

1. System structure

The above design scheme is implemented in a lab-scale DC motor drive system which is shown in Figure 4.24.

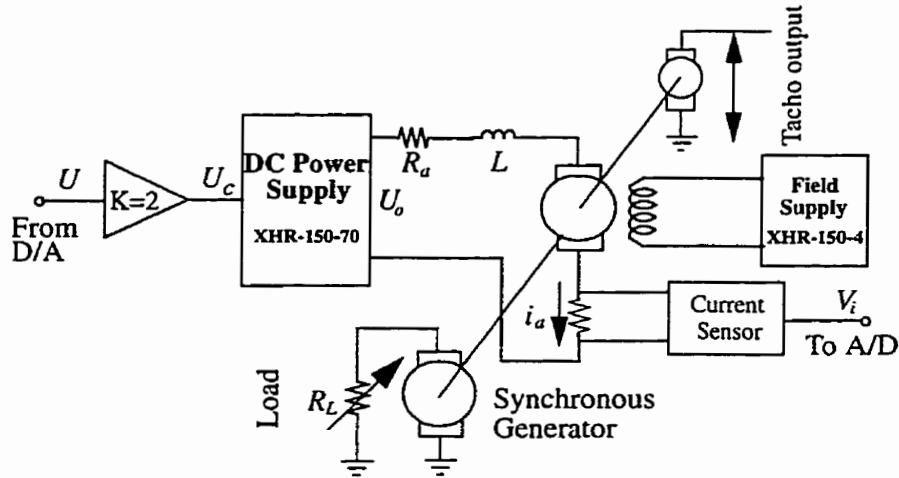


Figure 4.24 Open-loop DC motor drive system with current sensor

The related parameters of the system are:

Power Supply (XHR-150-70): $U_o = 15.1647 \cdot U_c - 0.2242$

Current sensor: $V_i = 1.6656 \cdot i_a - 0.0023$

L : The motor armature inductance (0.08 H)

R_a : The motor armature resistance (4.0 Ω)

J_M : The moment of inertia of the whole system (0.012 $\text{kg} \cdot \text{m}^2$)

f : The motor friction coefficient (0.002 $\text{N} \cdot \text{m} \cdot \text{s}/\text{rad}$)

$K_{m(e)}$: The motor voltage constant (0.46 $\text{V} \cdot \text{s}/\text{rad}$)

$K_{m(i)}$: The motor mechanical constant (0.46 $\text{N} \cdot \text{m}/\text{A}$)

K_s : The tacho speed-voltage constant (0.0215 V/rpm)

The armature circuit of the motor can be modelled as:

$$L \frac{di_a(t)}{dt} + R_a i_a(t) = u(t) + e_b(t) \quad (4.107)$$

where e_b is the back emf voltage, which is proportional to the motor speed as:

$$e_b(t) = K_{m(e)} \omega(t) \quad (4.108)$$

where ω is the angular speed of the motor. Taking into account the load disturbance, the mechanical governing equation of the system can be written as:

$$J_m \frac{d\omega(t)}{dt} + f\omega(t) = T_m(t) - T_d \quad (4.109)$$

where T_d is the constant load torque, and $T_m(t)$ is the motor generated torque which is:

$$T_m(t) = K_{m(t)} i_a(t) \quad (4.110)$$

By combining the above equations, the total dynamics of the motor can be modelled as:

$$\begin{bmatrix} \frac{di_a(t)}{dt} \\ \frac{d\omega(t)}{dt} \end{bmatrix} = \begin{bmatrix} -\frac{R_a}{L} & \frac{K_{m(e)}}{L} \\ \frac{K_{m(t)}}{J_m} & -\frac{f}{J_m} \end{bmatrix} \begin{bmatrix} i_a(t) \\ \omega(t) \end{bmatrix} + \begin{bmatrix} 1 \\ \bar{L} \\ 0 \end{bmatrix} \cdot u(t) + \begin{bmatrix} 0 \\ 1 \\ -\frac{1}{J_m} \end{bmatrix} \cdot T_d \quad (4.111)$$

By taking T_d as one of the system states, together with armature current and angular speed, the following state variables can be defined:

$$x(t) = \begin{bmatrix} i_a(t) & \omega(t) & T_d \end{bmatrix}^T \quad (4.112)$$

The system can then be represented as:

$$\begin{aligned} \dot{x}(t) &= \begin{bmatrix} -\frac{R_a}{L} & \frac{K_{m(e)}}{L} & 0 \\ \frac{K_{m(t)}}{J_m} & -\frac{f}{J_m} & -\frac{1}{J_m} \\ 0 & 0 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 1 \\ \bar{L} \\ 0 \end{bmatrix} u(t) \\ y(t) &= \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} x(t) \end{aligned} \quad (4.113)$$

Since the dynamics of the tacho generator are relatively fast in comparison with those of the rest of the system, it is also not unreasonable to assume that the tacho generator output is proportional to its speed as follows:

$$\omega_s = K_s \omega \quad (4.114)$$

where ω_s is the measured angular speed signal from tachometer, K_s can be interpreted as the sensor gain, and the sensor failure will result in changes in K_s .

By substituting the values of system parameters into EQ (4.113), the system can be described by:

$$\begin{aligned} \dot{x} &= \begin{bmatrix} -50 & -5.75 & 0 \\ 38.34 & -0.167 & -83.33 \\ 0 & 0 & 0 \end{bmatrix} x + \begin{bmatrix} 12.5 \\ 0 \\ 0 \end{bmatrix} u \\ y &= [0 \ 1 \ 0] x \\ \omega_s &= 0.0215 \cdot \omega \end{aligned} \quad (4.115)$$

To reduce the chance of common mode failures, it is highly desirable that the redundant sensors be something other than a mere replica of the existing tacho-generator. An effective way is to apply the concept of hybrid redundancy of Chapter 3, where the speed information is obtained through estimation based on the measurement from different parts of the system.

2. Closed-loop system structure and design

Knowing the analytic relationships among the motor speed, the armature voltage and current, one will be able to estimate the speed from the voltage and current signals. If the estimation from voltage and current is accurate enough, it can be regarded as redundant information. Since there are no mechanical 'moving' parts in the voltage and current transducers, generally, they are inherently more durable. Better still, we could even

easily use multiple voltage/current sensors followed by a voting scheme to further enhance the reliability of the measurement system. Therefore, in the analysis to follow, we will assume that the reliability of the voltage/current measurement devices is significantly higher than that of the tacho generator. Clearly, such redundancy consists of both physical and analytical elements.

A detailed block diagram of the control system is depicted in Figure 4.25. Based on the motor model, a state observer is used to estimate the motor speed signal, and the unknown load disturbance T_d . It should be mentioned that by estimating such unknown disturbance load, its effect can be eliminated.

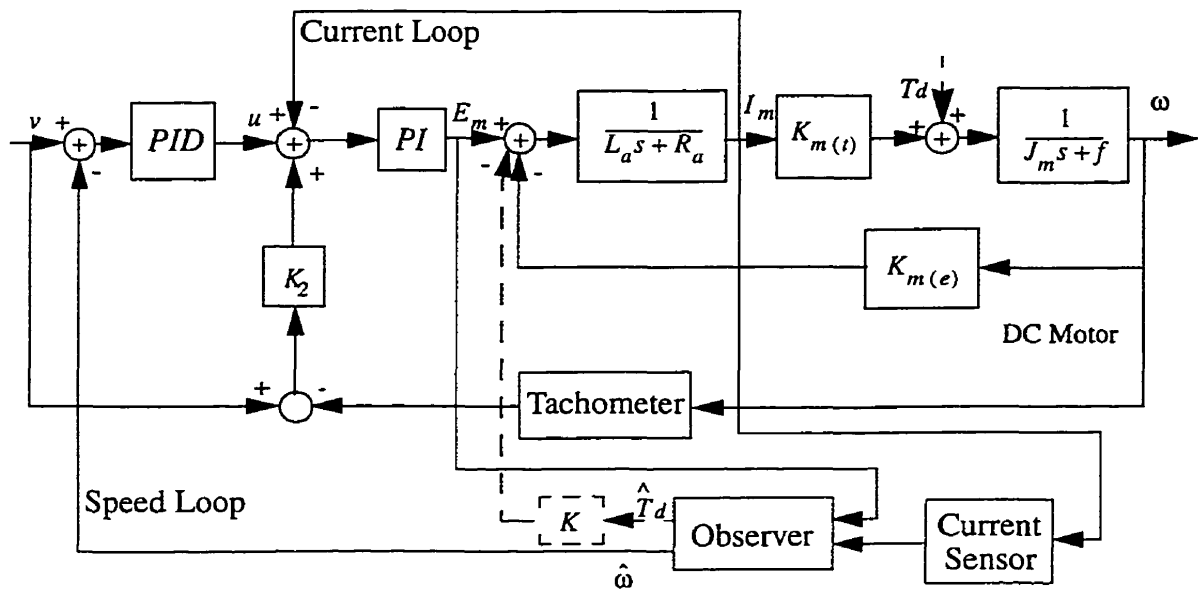


Figure 4.25 Reliable servo system structure

The observer used in Figure 4.25 is given as follows:

$$\dot{\hat{x}}(t) = \begin{bmatrix} -\frac{R_a}{L_a} & -\frac{K_m(e)}{L_a} & 0 \\ \frac{K_m(t)}{J_m} & \frac{f}{J_m} & -\frac{1}{J_m} \\ 0 & 0 & 0 \end{bmatrix} x(t) + \begin{bmatrix} \frac{1}{L_a} \\ 0 \\ 0 \end{bmatrix} u(t) + H \left(I_m(t) - \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \hat{x}(t) \right) \quad (4.116)$$

where $\hat{x}(t) = [\hat{I}_m(t) \ \hat{\omega}(t) \ \hat{T}_d(t)]$, $u(t) = E_m(t)$, and H is a 3×1 observer gain vector. By properly choosing H , the estimated states will converge to the real system states, i.e. $\hat{\omega}(t) \rightarrow \omega(t)$, and $\hat{T}_d \rightarrow T_d$ under the assumption that there is no modelling error in the observer.

3. Closed-loop system performance

To evaluate the effectiveness of this FTCS design approach, the performance of the drive system under the following three types of tacho generator failure modes have been considered:

- (1) reduction in the tacho effectiveness (reduction in the sensor gain);
- (2) poor calibration (tacho with an unknown bias); and
- (3) break in the tacho generator signal channel (total loss of the speed signal).

First of all, for the performance of the speed estimator, the estimated and the measured speed signals are compared in Figure 4.26 under normal operating conditions. It can be seen clearly that the state observer can indeed provide an accurate motor speed estimation.

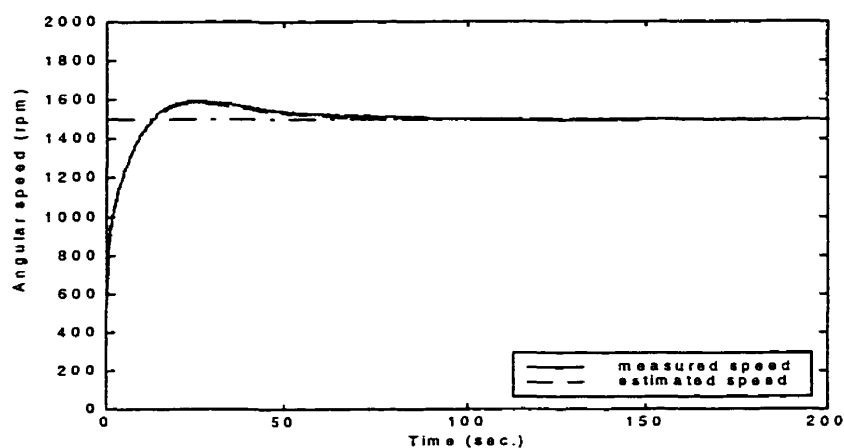


Figure 4.26 Comparison of the measured and the estimated motor speed

It is important to mention that, because the dynamics of the observer are extremely fast, there is no noticeable performance deterioration when the estimated speed signal is used for feedback purposes, rather than the measured speed signal. This is an important observation for the remainder of the experiments.

The speed regulation characteristics of the closed-loop system were then examined when the speed sensor suddenly loses its effectiveness by a 20% gain reduction. The results of the FTCS design and the conventional tacho based feedback control are illustrated in Figure 4.27. Clearly, in the case of FTCS design, the failure in the tacho only causes a negligible disturbance in the generator speed. However, in the case of conventional design, the failure has led to a 20% speed error.

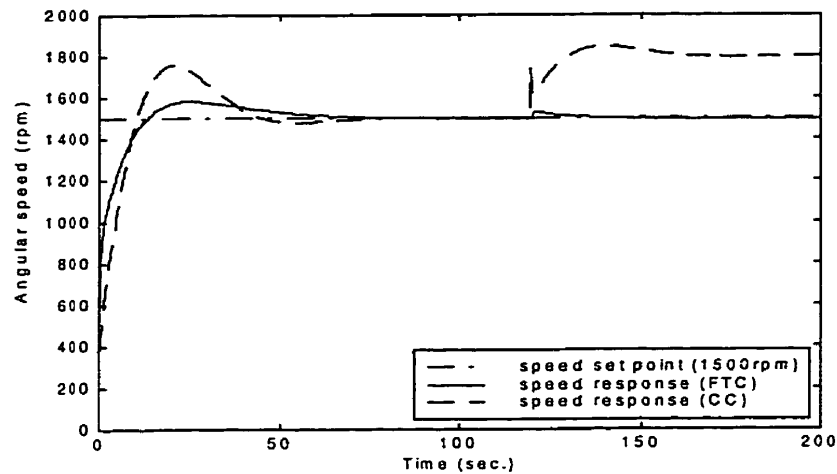


Figure 4.27 The performance of FTCS and the conventional design under the 20% reduction in the sensor effectiveness

One of the commonly occurring problems in measurement devices is bias. Due to the feedback nature of the control system, a minor bias can lead to a steady-state error in the controlled variable. As discussed in Chapter 2, effectively, a bias in the measurement can be considered as a fault. The performance of the FTCS design and that of the conventional design are compared in Figure 4.28 for the presence of 10% bias in the speed measurement. It can be seen clearly that the effect of the bias on the FTCS design is much smaller than that of the direct tacho feedback.

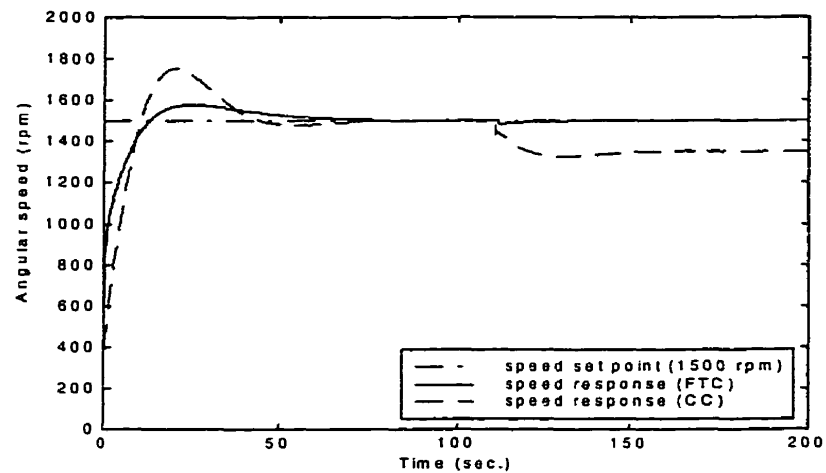


Figure 4.28 The performance of FTCS and the conventional design in the presence of +10% bias

One very serious type of fault in measurement devices is the total loss of the signal due to broken wires, power failure in transducers, etc. For the conventional tachometer feedback control, the entire system would become open-loop. However, using the current FTCS design, the speed signal can still be obtained from the current and voltage measurements. The performance of the FTCS system design and the conventional design is illustrated in Figure 4.29.

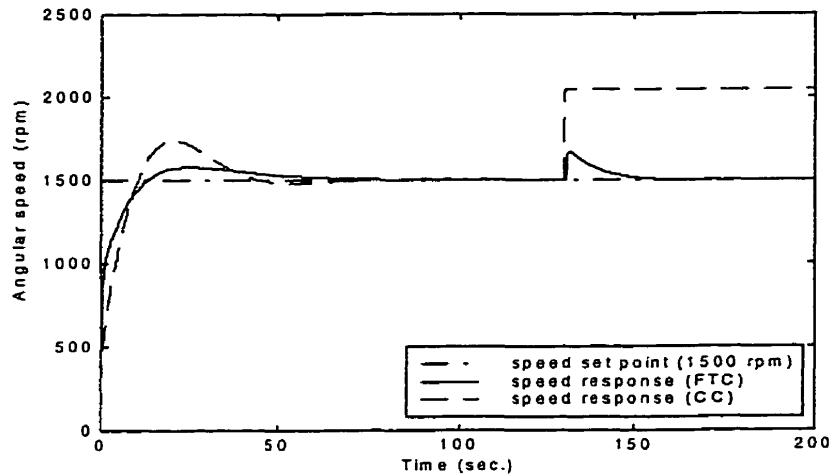


Figure 4.29 The performance of FTCS and the conventional design for the total loss of the tachometer generator signal

The experimental results have clearly demonstrated the robustness of the FTCS design against feedback sensor failures. One minor disadvantage of such a FTCS design is that the complexity of the system has increased. Furthermore, when the tachometer signal is totally lost, the system may no longer possess good load disturbance rejection properties.

4.5 Conclusion

In this chapter, passive FTCS design are discussed. Existing design methods are reviewed first. New design methods of passive FTCS against actuator and sensor failures are then proposed, where the actuator and sensor redundancies were utilized respectively to achieve the fault tolerance. The proposed designs were successfully applied to a ball-beam system and a lab-scale DC drive system, as well as simulated for an aircraft flight control system.

4.6 Bibliography

- [1] R. J. Veillette, J. V. Medanic and W. R. Perkins, "Design of reliable control systems," *IEEE Trans. on Automatic Control*, vol. 37, no. 3, pp. 290 -304, 1992.
- [2] E. Shimemura and M. Fujita, "A design method for linear state feedback systems possessing integrity based on a solution of a Riccati-type equation," *International Journal of Control*, vol. 42, no. 4, pp. 887-899, 1985.
- [3] J. J. Belletrutti and A. G. J. MacFarlane, "Characteristic loci techniques in multivariable control system design," *Proc. IEE*, vol. 118, no. 9, 1971, pp.1291-1297.
- [4] A. G. J. MacFarlane, *Complex Variable Methods for Linear Multivariable Feedback Systems*, London: Taylor and Francis Ltd., 1980.
- [5] M. Fujita and E. Shimemura, "Integrity against arbitrary feedback-loop failure in linear multivariable control systems," *Automatica*, vol. 24, no. 6, pp. 765-772, 1988.
- [6] L. S. Shieh, H. M. Dib, S. Ganesan and R. E. Yates, "Optimal pole-placement for state-feedback systems possessing integrity," *International Journal of Systems Science*, vol. 19, no. 8, pp. 1419-1435, 1988.
- [7] B. D. O. Anderson and J. B. Moore, *Optimal Control: Linear Quadratic Methods*, Prentice-Hall, Englewood Cliffs, NJ, 1990.
- [8] S. M. Joshi, "Design of failure-accommodation multiloop LQG-type controllers," *IEEE Trans. on Automatic Control*, vol. 32, no. 8, pp. 740-741, 1987.
- [9] R. J. Veillette, "Reliable linear quadratic state-feedback control," *Automatica*, Vol. 31, No. 1, pp. 137-143, 1995.
- [10] D. D. Siljak, "Dynamic reliability using multiple control system," *Proceedings of the 2nd Lawrence Symposium on Systems and Decision Sciences*, Berkeley, CA, pp. 173 - 187, 1978.

- [11] D. D. Siljak, *Decentralized Control of Complex Systems*, Academic Press, Inc., UK., 1991.
- [12] M. Vidyasagar and N. Viswanadham, "Algebraic design techniques for reliable stabilization," *IEEE Trans. on Automatic Control*, vol. AC-27, pp. 1085-1095, 1982.
- [13] M. H. Shor, W. R. Perkins, and J. V. Medanic, "Design of reliable decentralized controllers: a unified continuous/discrete formulation," *International Journal of Control*, vol. 56, no. 4, pp. 943-965, 1992.
- [14] D. D. Siljak, "Parameter space methods for robust control design: a guided tour," *IEEE Trans. Automatic Control*, vol. AC-34, no. 7, pp. 674-688, 1989.
- [15] J. E. Ackermann, *Robust Control: Systems with Uncertain Physical Parameters*, Springer-Verlag, New York, 1993.
- [16] E. J. Davison, "The robust control of a servomechanism problem for linear time-invariant multivariable systems," *IEEE Trans. Automatic Control*, vol. AC-21, pp. 25-34, 1976.
- [17] B. R. Barmish and H. I. Kang, "A survey of extreme point results for robustness of control systems," *Automatica*, vol. 29, no. 1, pp. 13-35, 1993.
- [18] C. B. Soh, H. C. Goh and C. K. Teo, "Invariance of the dynamic properties of a linear continuous time system," *International Journal of Systems Science*, vol. 22, no. 9, pp. 1637-1646, 1991.
- [19] K. Suyama, "A new type of reliable control system using decision by majority", *Electronics and Communications in Japan*, Part2, vol. 81, no. 2, pp. 46 - 54, 1998.
- [20] R. N. Clark, "State estimation schemes for instrument fault detection," in *Fault Diagnosis in Dynamic Systems, Theory and Applications*, (edited by R. Patton, P. M. Frank and R. Clark), Prentice Hall, New York, 1989.

- [21] N. Matsui, "Sensorless PM brushless DC motor drives," *IEEE Trans. Ind. Electron.*, vol. 43, no. 2, 1996.
- [22] T. H. Lee, T. S. Low, K. J. Tseng and H. K. Lim, "An intelligent indirect dynamic torque sensor for permanent magnet brushless DC drives," *IEEE Trans. Ind. Electron.*, vol. 41, no. 2, 1994.

Fault Detection and Identification[†]

5.1 Introduction

In the preceding chapter, design issues of the passive fault tolerant control have been thoroughly examined. Beginning with this chapter, the design of active fault tolerant control systems will be discussed. It is known that the design of active FTCS involves two steps: one is to design a Fault Detection and Identification (FDI) scheme, and the other is to design a Reconfigurable Control Scheme (RCS). The role of the first step is to detect the occurrence of faults/failures in the system and obtain information on the faults and the faulty system; in the second step, based on the FDI information, the controller parameters are reconfigured to maintain appropriate control over the post-fault system.

In this chapter, the design of FDI schemes will be considered. First, concepts and principles of FDI are described along with an introduction to the basic design techniques. Finally, a FDI scheme using a bounding parameter estimation algorithm is proposed for the integrated design of active FTCS.

[†] : A version of this chapter has been submitted for publication:

J. Jiang and Q. Zhao, "Comparison of RLS parameter and state estimation based FDI schemes," submitted to *Journal of Franklin Institute* in January, 1999.

5.2 Principles of FDI

Since FDI is a very important step for achieving fault tolerance in automatic systems and processes, it has drawn extensive research interest and a lot of progress has been made in recent years. A variety of design techniques have been developed and successfully applied [1] [2] [3]. Among the existing techniques, model-based approaches play an important role. As the name implies, such methods carry out FDI tasks based on the mathematical model of the system. Three types of commonly used model-based FDI techniques are based on: (1) state estimation; (2) parameter estimation; and (3) parity space. It should be mentioned that only state estimation based and parameter estimation based FDI schemes are considered in this thesis.

The basic idea of FDI is to generate a residual signal which is sensitive to the occurrence of the fault, and then perform a hypothesis test on the residual signal to determine the fault occurrence and finally identify the source and the size of the fault.

It is important to emphasize that, for a given FDI task, the amount of information available to all model-based FDI methods is the same, i.e. complete knowledge of the pre-fault system and the set of input-output data. The only difference among various methods is how such information is used.

In state estimation based FDI approaches, a state estimator (an observer or a Kalman filter) is synthesized for the purpose of residual generation. If the system operates normally, the residual of the estimator should be very small (or a white noise process in stochastic case). If a fault has occurred, the residual will be large (or non-white). Therefore, the fault can be detected by performing a hypothesis test on the residual signal. In parameter estimation based FDI approaches, the system parameters are estimated on-line in real-time. Once the parameter estimates have converged, they are then compared with the nominal parameters to generate the residual. In the absence of system faults, this signal should be close to zero, or very “small”. Otherwise, if a fault has occurred, the residual

signal will be relatively “large”. Hence, FDI can be carried out simply by checking the parameter discrepancies. A parity space based FDI approach relies on checking the cause-effect relationships between the system input and output. If the system operates normally, the input-output data should match the mathematical model of the system, otherwise, this matching condition will no longer hold.

Because different FDI schemes use different residual generating mechanisms, their performance will be different even under the same fault scenario. Several attempts have been made recently to explore the similarities and differences among the above-mentioned FDI approaches. It has been shown that the discrete parity space method is exactly the same as a deadbeat observer, [4]. The relationship between the parity space and the parameter estimation has been investigated in [5]. Comparisons have been made between the parameter estimation and the observer based approaches in [6] [7]. Some new results on the relationships between these two approaches have been obtained through the application of a parametric observer, [8]. Different types of residual generation schemes for FDI have also been investigated in a unified way in [9].

In active FTCS, the efficiency of the FDI scheme has a direct effect on the reconfigurable control. The fast detection and accurate fault information provided by FDI will help the RCS to take proper control action in time so that the system stability and performance can be maintained. In this sense, an effective FDI scheme can benefit the performance of the entire system. The design of FDI and RCS should not be conducted separately, and they shall cooperate to “fight” against faults/failures in an integrated manner. Therefore, the FDI scheme should be designed in such a way that it can be readily integrated with the reconfigurable control scheme.

5.3 State Estimation Based FDI

5.3.1 Residual generation using observers or Kalman filters

The basic principle of residual generation using state estimation is illustrated in Figure 5.1.

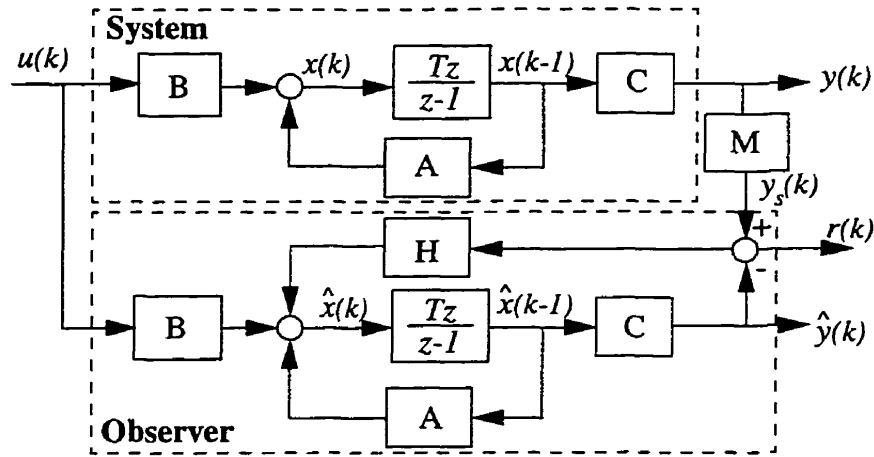


Figure 5.1 Residual generation using an observer

In this figure, M represents the sensors. The relationship between output matrix C and measurement matrix M has been illustrated in Chapter 2. The measured system variable $y_s(k)$, is compared with the corresponding signals from the observer/Kalman filter, $\hat{y}(k)$ to generate the residual signal:

$$r(k) = y_s(k) - \hat{y}(k) = My(k) - \hat{y}(k) \quad (5.1)$$

The residual calculated in EQ (5.1) also represents the observation error and is fed back to the observer to improve the state estimation. If there is no fault in the system, the residual signal $r(k)$ will only reflect the system measurement noise or other unmodelled disturbances in the system. However, if a fault has occurred in the system, the model

of the observer will no longer match the actual system, the magnitude of the residual signal $r(k)$ will then increase. Therefore, by checking this residual signal, faults can be detected.

Consider a linear SISO system with the following model representation:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) + v(k) \end{aligned} \quad (5.2)$$

where $x(k) \in \mathbb{R}^{n \times 1}$ is the state variable, $y(k) \in \mathbb{R}^{1 \times 1}$ is the system output and $v(k)$ is the measurement noise with the covariance defined by:

$$E[v(k)v(j)] = \sigma^2 \delta_{kj} \quad (5.3)$$

where δ_{kj} is the Kronecker delta function.

$$A = \begin{bmatrix} 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & 0 & \dots & 0 & 1 \\ -a_n & -a_{n-1} & \dots & -a_2 & -a_1 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \dots \\ 1 \end{bmatrix} \quad C = [b_n \ b_{n-1} \ \dots \ b_1] \quad (5.4)$$

The sensor output is written as:

$$y_s(k) = My(k) \quad (5.5)$$

Since no redundant sensor is considered here, the dimension of $y_s(k)$ is equal to that of system output, $y(k)$. Therefore, for the above system, $M = 1$ during normal system operation.

When the measurement noise is negligible, a full order observer can be used to generate the residual signal:

$$\begin{aligned}\hat{x}(k+1) &= A\hat{x}(k) + Bu(k) + H[y_s(k) - \hat{y}(k)] \\ \hat{y}(k) &= C\hat{x}(k)\end{aligned}\tag{5.6}$$

$\hat{x}(k) \in \mathbb{R}^{n \times 1}$ and $\hat{y}(k) \in \mathbb{R}^{1 \times 1}$ are the estimated system states and output, respectively. The vector $H \in \mathbb{R}^{n \times 1}$ is known as the observer gain which can be designed to achieve the desired rate of convergence of the observer.

With the state estimation error denoted as $e(k) = x(k) - \hat{x}(k)$, in the absence of faults, it can be calculated as:

$$e(k+1) = (A - HC)e(k)\tag{5.7}$$

or,

$$e(k) = (A - HC)e(k-1) = (A - HC)^{k-k_0}e(k_0)\tag{5.8}$$

where k_0 is the initial time instant.

If the observer gain is chosen such that the eigenvalues of the matrix $(A - HC)$ satisfy the following condition:

$$\max_i |\lambda_i(A - HC)| = \mu < 1\tag{5.9}$$

the norm of the estimation error will approach to zero exponentially if there is no fault in the system, i.e.

$$\lim_{k \rightarrow \infty} \|e(k)\| \leq \lim_{k \rightarrow \infty} \delta \mu^{k-k_0} \|e(k_0)\| \rightarrow 0\tag{5.10}$$

where δ is a positive constant.

If the measurement noise cannot be neglected, Kalman filters can be used for residual generation in this case:

$$\hat{x}(k+1|k+1) = \hat{x}(k+1|k) + \tilde{K}(k+1) [y_s(k+1) - C\hat{x}(k+1|k)] = \quad (5.11)$$

$$\hat{x}(k+1|k) = A\hat{x}(k|k) + Bu(k) \quad (5.12)$$

and

$$\hat{y}(k) = C\hat{x}(k|k) \quad (5.13)$$

where $\hat{x}(k+1|k)$ denotes the conditional mean of $x(k+1)$ given observations of $\{y(i)\}, i = 1, 2, \dots, k$.

The Kalman filter gain, $\tilde{K}(k+1)$, is obtained from:

$$\tilde{K}(k+1) = \Sigma(k+1|k) C^T (C\Sigma(k+1|k) C^T + \sigma^2)^{-1} \quad (5.14)$$

The *a priori* estimation error covariance matrix $\Sigma(k+1|k) = E[e(k+1|k) e^T(k+1|k)]$ is calculated as:

$$\begin{aligned} \Sigma(k+1|k) = & A\Sigma(k|k-1)A^T \\ & - A\Sigma(k|k-1)C^T(C\Sigma(k|k-1)C^T + \sigma^2)^{-1}C\Sigma(k|k-1)A^T \end{aligned} \quad (5.15)$$

where the *a priori* estimation error is defined as:

$$e(k+1|k) = x(k+1) - \hat{x}(k+1|k) \quad (5.16)$$

It has been proven that $\hat{x}(k+1|k)$ is the minimum variance estimator if the measurement noise is Gaussian, [10] [11]. The expected value of the estimation error will be:

$$E[e(k+1|k) | \{y(i), i = 1, 2, \dots, k\}] = 0 \quad (5.17)$$

and the error covariance matrix $E[e(k+1|k) e^T(k+1|k) | \{y(i), i = 1, 2, \dots, k\}]$ is minimum compared to that of other estimators.

By substituting EQ(5.11) into EQ (5.12), one can obtain another form of Kalman filter:

$$\hat{x}(k+1|k) = A\hat{x}(k|k-1) + Bu(k) + K(k) (y_s(k) - C\hat{x}(k|k-1)) \quad (5.18)$$

where the Kalman filter gain is calculated from:

$$K(k) = A\tilde{K}(k) \quad (5.19)$$

From EQ (5.2) and EQ (5.18), one can obtain that:

$$e(k+1|k) = (A - K(k)C) e(k|k-1) - K(k)v(k) \quad (5.20)$$

The rate of convergence of $e(k+1|k)$ depends on the eigenvalues of the following matrix:

$$\Psi(k) = A - K(k)C \quad (5.21)$$

This matrix is time-varying due to $K(k)$. A lot of research has been done to study how the matrix $\Psi(k)$ behaves when $K(k)$ is updated using EQs (5.14) & (5.15), [10] [11]. In fact, the Kalman filter gain $K(k)$ and the *a priori* estimation error covariance matrix $\Sigma(k+1|k)$ converge to their steady-state values as $k \rightarrow \infty$. From EQ (5.15), as $\Sigma(k+1|k)$ converges, its steady-state value $\Sigma = \lim_{k \rightarrow \infty} \Sigma(k+1|k)$ satisfies the following algebraic Riccati equation:

$$\Sigma - A\Sigma A^T + A\Sigma C^T (C\Sigma C^T + \sigma^2)^{-1} C\Sigma A^T = 0 \quad (5.22)$$

Based on the solution of the above equation, the steady-state Kalman filter can be obtained from the following lemma, [10].

Lemma 5.1 *If the system is stabilizable, and the pair (C, A) is observable, then*

(1) $K(k) \rightarrow K_{ss}$ exponentially, where K_{ss} is known as the steady-state Kalman filter gain, and

(2) $\Psi(k) \rightarrow \Psi_{ss}$ exponentially, where $\Psi_{ss} = A - K_{ss}C$ is the steady-state transition matrix that has all eigenvalues inside the unit circle, i.e:

$$|\lambda_i \{\Psi_{ss}\}| \leq 1 \quad (5.23)$$

Since the state estimation error equation can be rewritten as:

$$e(k+1|k) = \prod_{i=k_0}^k (A - K(i)C) e(k_0) - \sum_{j=k_0}^k (A - K(j)C)^j K(k-j) v(k-j) \quad (5.24)$$

where $e(k_0) = x(k_0) - \hat{x}(k_0)$, Lemma 5.1 implies that the state estimation error converges to zero exponentially, i.e.,

$$\lim_{k \rightarrow \infty} \|E[e(k+1|k)]\| < \lim_{k \rightarrow \infty} \left\| \prod_{i=k_0}^k (A - K(i)C) \right\| \|e(k_0)\| \rightarrow 0 \quad (5.25)$$

5.3.2 Observer/Kalman filter based fault detection

Generally speaking, faults in a dynamic system are often associated with malfunction of system components, which are reflected as changes in the system parameters. Therefore, system dynamic faults can be modelled as parameter changes.

For the system described in EQ (5.2), according to the fault models in Chapter 2, the faults can be represented in a multiplicative form:

$$(A, B) = \begin{cases} (A_o, B_o) & k < k_f \quad \text{No Fault} \\ (A_o + \Delta A, B_o + \Delta B) & k \geq k_f \quad \text{Fault} \end{cases} \quad (5.26)$$

or an additive form, i.e. a sensor bias:

$$y_s(k) = \begin{cases} y(k) & k < k_f \quad \text{NoFault} \\ L_s y(k) + f_s(k) & k \geq k_f \quad \text{Fault} \end{cases} \quad (5.27)$$

where (A_o, B_o) are the nominal system matrices, and $(\Delta A, \Delta B)$ are their fault-induced changes. L_s represents faults induced change in the sensor gain, and $f_s(k)$ is the sensor bias.

In the observer case, when the system is fault-free, the residual signal is:

$$\begin{aligned} r(k) &= y_s(k) - \hat{y}(k) \\ &= My(k) - \hat{y}(k) \\ &= Ce(k) + (M-1)Cx(k) \end{aligned} \quad (5.28)$$

Notice that $M = 1$ when the sensor functions normally, the residual signal can further be written as:

$$r(k) = Ce(k) = C(A-HC)^{k-k_0} e(k_0) \quad (5.29)$$

From EQ (5.10), in the absence of measurement noise and any faults, the residual signal $r(k)$ generated by the observer goes to zero exponentially, i.e. $r(k) \rightarrow 0$.

Once the fault occurs at the time instant k_f , the equation governing the state estimation error becomes:

$$\begin{aligned} e(k) &= (A-HC)e(k-1) + \Delta Ax(k-1) + \Delta Bu(k-1) + Hf_s(k-1) \\ &= (A-HC)e(k-1) + f_o(k-1) \end{aligned} \quad k > k_f \quad (5.30)$$

where $f_o(k) = \Delta Ax(k) + \Delta Bu(k) + Hf_s(k)$ appears to be an additional term in the system equation, which contains all fault induced changes.

The estimation error can then be calculated as:

$$e(k) = (A - HC)^{k-k_f} e(k_f) + \sum_{i=k_f+1}^k (A - HC)^{k-i} f_o(i-1) \quad k > k_f \quad (5.31)$$

Since $e(k_f) = (A - HC)^{k_f-k_0} e(k_0)$, therefore, one can have:

$$e(k) = (A - HC)^{k-k_0} e(k_0) + \sum_{i=k_f+1}^k (A - HC)^{k-i} f_o(i-1) \quad k > k_f \quad (5.32)$$

Therefore, the residual signal in this case becomes:

$$\begin{aligned} r(k) &= y_s(k) - \hat{y}(k) \\ &= Ce(k) + f_s(k) \\ &= C(A - HC)^{k-k_0} e(k_0) + \sum_{i=k_f+1}^k C(A - HC)^{k-i} f_o(i-1) + f_s(k) \end{aligned} \quad (5.33)$$

It should be noted that the fault induced term $f_o(k)$ acts as an external input to the state estimator. Although as $k \rightarrow \infty$, the first term in EQ (5.33) converges to zero, the residual signal in EQ (5.33) will no longer be zero and can be used to detect the fault occurrence. Due to the exponential convergence of the first term, the transients of the residual signal dies out quickly, and it will reach a steady-state that reflects the scale of the fault.

In the case of Kalman filters, when the system operates normally, the residual signal is calculated as follows:

$$r(k) = y_s(k) - C\hat{x}(k|k-1) = Ce(k|k-1) + v(k) \quad k \leq k_f \quad (5.34)$$

which is a zero mean white Gaussian noise with the known covariance as:

$$\begin{aligned}
R(k) &= E[r(k) r^T(k)] \\
&= E\{[Ce(k|k-1) + v(k)][Ce(k|k-1) + v(k)]^T\} \\
&= C\Sigma(k|k-1)C^T + \sigma^2
\end{aligned} \tag{5.35}$$

If a fault has occurred in the system as in EQs (5.26) & (5.27), the residual signal becomes:

$$r(k) = Ce(k|k-1) + v(k) + f_s(k) \quad k \geq k_f \tag{5.36}$$

with

$$e(k|k-1) = (A - K(k-1)C)e(k-1|k-2) + K(k-1)v(k-1) + f_n(k-1) \quad k \geq k_f \tag{5.37}$$

where $f_n(k) = \Delta Ax(k) + \Delta Bu(k) + K(k)f_s(k)$ contains the fault induced changes.

In this case, $r(k)$ is no longer a zero-mean white Gaussian noise, the fault detection can be carried out by analyzing the change in the characteristics of $r(k)$ through proper statistical tests, such as tests of whiteness, tests of mean and tests of covariance, [12][13]. One way to do it is to construct the following variable:

$$l(k) = \sum_{i=k-N+1}^k r^T(i) R^{-1}(i) r(i) \tag{5.38}$$

where $R(i)$ is the covariance matrix of the residual signal as in EQ (5.35).

It is well known that $l(k)$ is a random variable with a χ^2 distribution in the normal case. Then, the fault detection can be achieved by the following hypothesis test:

$$\begin{aligned}
H_0 \quad & l(k) \leq \gamma_o \quad \text{No Faults} \\
H_1 \quad & l(k) > \gamma_o \quad \text{Faults}
\end{aligned} \tag{5.39}$$

When choosing the threshold γ_o and the window length N , one has to take consideration of the issues of detection delay, probability of missing detection and false alarm. Usually, there exists certain trade-off among these criteria, [14].

5.4 Parameter Estimation Based FDI

5.4.1 Residual generation using parameter estimation schemes

The residual generation scheme based on parameter estimation is depicted in Figure 5.2. Since many plant faults appear as changes in the system parameters, it is natural to make use of such information for fault detection. As shown in the figure, one can estimate system parameters in real-time and compare them with those from the off-line calculated nominal system model. The residual signal can then be used to detect the fault.

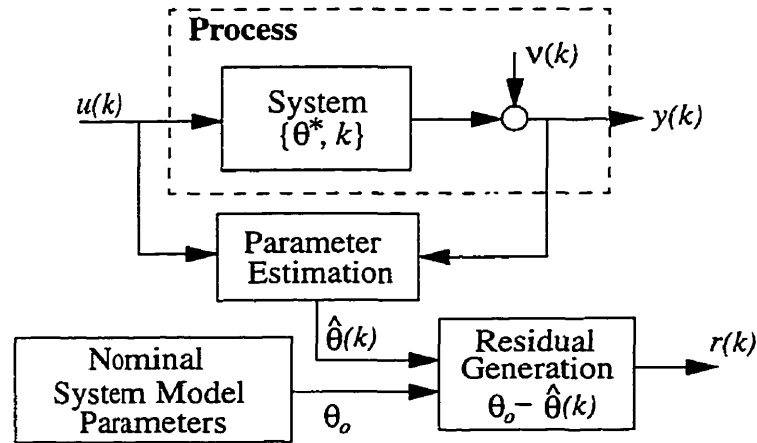


Figure 5.2 Residual generation using parameter estimation scheme

An n -th order linear time-invariant SISO system shown in EQ (5.2) can also be represented by the following ARMA model:

$$\begin{aligned}
 z(k) + a_1 z(k-1) + a_2 z(k-2) + \dots + a_n z(k-n) &= b_1 u(k-1) + \dots + b_n u(k-n) \\
 y(k) &= z(k) + v(k)
 \end{aligned}
 \tag{5.40}$$

or as:

$$y(k) = \psi^T(k) \theta^* + \omega(k) \tag{5.41}$$

where $u(k)$ and $y(k)$ are the system input and output, respectively, and $\theta^* = [a_1, \dots, a_n, b_1, \dots, b_n]^T \in \mathbb{R}^{2n}$ represents actual system parameters. $\psi(k)$ is the regression vector, $\psi^T(k) = [-y(k-1), -y(k-2), \dots, -y(k-n), u(k-1), \dots, u(k-n)] \in \mathbb{R}^{2n}$. $\omega(k)$ is so-called equation error, and $\omega(k) = v(k) + \sum_{i=1}^n a_i v(k-i)$. The measurement noise $v(k)$ (if present) is assumed to have a white Gaussian distribution with zero mean and a known variance: σ^2 .

It should be mentioned that the above ARMA model is equivalent to the system state-space representation in EQ (5.2), i.e. the parameters in both models are exactly the same. However, it is clear that the dimension of the ARMA model is $2n$, and that of the state-space representation is n .

From the input-output data and the ARMA model of EQ (5.41), a Recursive Least Square (RLS) parameter estimation scheme is used to estimate system parameters in order to achieve the real-time estimation:

$$\hat{\theta}(k) = \hat{\theta}(k-1) + P(k) \psi(k) [y(k) - \psi^T(k) \hat{\theta}(k-1)] \tag{5.42}$$

where $\hat{\theta}(k)$ is the estimated parameter vector, and the error covariance matrix is given as:

$$P(k) = \left[P(k-1) - \frac{P(k-1) \psi(k) \psi^T(k) P(k-1)}{1 + \psi^T(k) P(k-1) \psi(k)} \right] \tag{5.43}$$

$P(k) \in \Re^{2n \times 2n}$ is a positive definite symmetric matrix that can also be written as:

$$P^{-1}(k) = \sum_{i=1}^k \psi(i) \psi^T(i) = P^{-1}(k-1) + \psi(k) \psi^T(k) \quad (5.44)$$

In order to obtain the inverse matrix of $P(k)$, the system input signal $u(k)$ should be persistently excited to the order of, at least, $2n$, [15].

It is interesting to mention that both Kalman filters and RLS parameter estimation schemes use the same type of optimization criteria: least squares. The difference is that the former is to minimize the estimation error of the system states, while the latter is to minimize the estimation error of the system parameters.

Once the parameter estimates have converged, the following residual signal can be used for FDI purposes:

$$r_p(k) = [\theta_o - \hat{\theta}(k)]^T [\theta_o - \hat{\theta}(k)] \quad (5.45)$$

To achieve the minimum delay in fault detection, the convergence rate of the parameter estimate becomes one of the most important considerations.

1. Convergence analysis of RLS algorithm in the noise free situation

In the absence of measurement noise, EQ (5.42) can be written as:

$$\hat{\theta}(k) = \hat{\theta}(k-1) + P(k) \psi(k) [\psi^T(k) \theta^* - \psi^T(k) \hat{\theta}(k-1)] \quad (5.46)$$

Subtracting the true system parameter vector θ^* on both sides, it follows that:

$$[\theta^* - \hat{\theta}(k)] = [\theta^* - \hat{\theta}(k-1)] - P(k) \psi(k) \psi^T(k) [\theta^* - \hat{\theta}(k-1)] \quad (5.47)$$

or in a more compact form as:

$$\tilde{\theta}(k) = [I - P(k) \psi(k) \psi^T(k)] \tilde{\theta}(k-1) \quad (5.48)$$

EQ (5.48) represents an autonomous time-varying system of order $2n$ whose state is the parameter estimation error vector, $\tilde{\theta}(k) = \theta^* - \hat{\theta}(k)$. The one-step state transition matrix can be shown as:

$$\begin{aligned} \Phi(k, k-1) &= I - P(k) \psi(k) \psi^T(k) \\ &= P(k) [P^{-1}(k) - \psi(k) \psi^T(k)] \\ &= P(k) P^{-1}(k-1) \end{aligned} \quad (5.49)$$

Consequently, the parameter estimation error will become:

$$\tilde{\theta}(k) = \Phi(k, k_0) \tilde{\theta}(k_0) = P(k) P^{-1}(k_0) \tilde{\theta}(k_0) \quad (5.50)$$

where k_0 is the initial time step.

For given $P^{-1}(k_0)$ and $\tilde{\theta}(k_0)$, the convergence of the parameter estimation error is a sole function of $P(k)$, which can be analyzed using the following lemma.

Lemma 5.2 *If the system is persistently excited, then, the norm of the parameter estimation error in EQ (5.50) converges to zero, i.e. $\|\tilde{\theta}(k)\| \rightarrow 0$, at the rate of $(1/k)$.*

Proof:

With a persistently exciting system input, one can define the following matrix:

$$G = \lim_{k \rightarrow \infty} \frac{1}{k} \left(\sum_{i=1}^k \psi(i) \psi^T(i) \right) = \lim_{k \rightarrow \infty} \frac{1}{k} P^{-1}(k) \quad (5.51)$$

The elements in G are auto-correlation and cross-correlation terms of the system input and output. If the nominal system is stable, and the persistent excitation condi-

tion is satisfied, G is a positive definite matrix whose elements are bounded. Hence, it follows that:

$$\lim_{k \rightarrow \infty} P(k) = \lim_{k \rightarrow \infty} \frac{1}{k} G^{-1} \quad (5.52)$$

and

$$\lim_{k \rightarrow \infty} \|P(k)\| = \lim_{k \rightarrow \infty} \frac{1}{k} \|G^{-1}\| \rightarrow 0 \quad (5.53)$$

Finally, the convergence of the estimation error can be shown as:

$$\lim_{k \rightarrow \infty} \|\tilde{\theta}(k)\| \leq \lim_{k \rightarrow \infty} \|P(k)\| \|P^{-1}(k_f)\| \|\tilde{\theta}(k_f)\| = \lim_{k \rightarrow \infty} \frac{1}{k} \|G^{-1}\| \|P^{-1}(k_f)\| \|\tilde{\theta}(k_f)\| = 0 \quad (5.54)$$

It is clear that the rate of convergence of $\|\tilde{\theta}(k)\|$ is only $(1/k)$. Hence the proof.

2. Convergence analysis of RLS algorithms in the presence of noise

If the measurement noise is non-negligible, one has to analyze the convergence of the algorithm statistically. From EQ (5.41), it is known that the equation error is a correlated process:

$$\omega(k) = y(k) - \psi^T(k) \theta^* = v(k) + \sum_{i=1}^n a_i v(k-i) \quad (5.55)$$

where $\omega(k)$ is a zero mean, but correlated Gaussian process with the variance:

$$\text{var}(\omega) = \sigma^2 \left(1 + \sum_{i=1}^n a_i^2 \right) \quad (5.56)$$

In this case, the equation governing the parameter estimation error vector will no longer represent an autonomous system. Instead, it has a noise driving term:

$$\tilde{\theta}(k) = \Phi(k, k-1) \tilde{\theta}(k-1) - P(k) \psi(k) \omega(k) \quad (5.57)$$

Following the previous analysis, it is easy to show that:

$$\begin{aligned} \tilde{\theta}(k) &= \Phi(k, k-1) \tilde{\theta}(k-1) - \sum_{l=1}^k \left\{ \prod_{i=l+1}^k [I - P(i) \psi(i) \psi^T(i)] P(i) \psi(i) \omega(i) \right\} \\ &= P(k) P^{-1}(k_0) \tilde{\theta}(k_0) - \sum_{l=1}^k P(k) P^{-1}(l) P(l) \psi(l) \omega(l) \\ &= P(k) P^{-1}(k_0) \tilde{\theta}(k_0) - P(k) \sum_{l=1}^k \psi(l) \omega(l) \end{aligned} \quad (5.58)$$

The first term in the above equation converges to zero at the rate of $(1/k)$. As for the second term, because $\omega(k)$ correlates with the first n terms in $\psi(k)$, in general, $E[\psi(k) \omega(k)] \neq 0$, i.e.

$$\begin{aligned} \lim_{k \rightarrow \infty} P(k) \sum_{l=1}^k \psi(l) \omega(l) &= \lim_{k \rightarrow \infty} \frac{1}{k} G^{-1} \sum_{l=1}^k \psi(l) \omega(l) \\ &= G^{-1} \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{l=1}^k \psi(l) \omega(l) \\ &= G^{-1} E[\psi \omega] \neq 0 \end{aligned} \quad (5.59)$$

In fact, EQ (5.59) states one well-known result of least squares based parameter estimation: even though the measurement noise is white, the correlated equation error may still lead to biased parameter estimates. In FDI applications, the biased parameter estimate is certainly undesirable because the bias may be mistakenly interpreted as the fault-induced parameter change, which will increase the probability of the false alarm. The bias problem can be dealt with either by using more robust parameter estimation schemes, or by taking the bias into account when selecting the threshold at the FDI decision-making stage.

5.4.2 RLS parameter estimation based fault detection

In the ARMA model representation, faults are modelled as parameter changes as shown in EQ (2.12). The system parameters can be written as:

$$\theta^* = \begin{cases} \theta & k < k_f \\ \theta + \Delta\theta & k \geq k_f \end{cases} \quad (5.60)$$

where $\theta = [a_1 a_2 \dots a_n b_1 \dots b_n]^T$ and $\Delta\theta = [\Delta a_1 \Delta a_2 \dots \Delta a_n \Delta b_1 \dots \Delta b_n]^T$ represent the nominal system parameter and the fault induced parameter changes, respectively. k_f is the fault occurrence time. For the sensor bias at the measured system output, the fault is similarly modelled in EQ (5.27).

For faults that result in system parameter changes, the convergence of the parameter estimates implies that:

$$\hat{\theta}(k) \rightarrow \begin{cases} \theta & \text{No Fault} \\ \theta + \Delta\theta & \text{Fault} \end{cases} \quad (5.61)$$

The fault detection can be achieved by testing the residual in EQ (5.45).

If the noise is negligible, to detect a fault, one only has to test for the non-zero value of ϵ_p :

$$\epsilon_p = (\theta - \hat{\theta})^T (\theta - \hat{\theta}) = \begin{cases} 0 & \text{No Fault} \\ \|\Delta\theta\|^2 \neq 0 & \text{Fault} \end{cases} \quad (5.62)$$

It is extremely important to note that the test of $\epsilon_p(k)$ is meaningful only after the parameter estimate, $\hat{\theta}(k)$, has converged to the true value. This is because other fac-

tors such as transients of the parameter estimates, or system disturbances, can also cause the non-zero value of $\varepsilon_p(k)$.

In the presence of noise, ε_p will satisfy a certain statistical distribution. For example, for white Gaussian noise, ε_p will have a χ^2 distribution. For a given probability of false alarm or missing detection, a suitable threshold γ_p can be determined. The fault detection then becomes the following hypothesis test [13]:

$$\begin{array}{lll} H_0 & \varepsilon_p \leq \gamma_p & \text{No Fault} \\ H_1 & \varepsilon_p > \gamma_p & \text{Fault} \end{array} \quad (5.63)$$

Isolation of multiplicative faults can be achieved by comparing the estimated and the nominal system parameters after the convergence of the parameter estimates:

$$\Delta\theta = \hat{\theta}(k) - \theta \approx [\Delta a_1, \Delta a_2, \dots, \Delta a_n, \Delta b_1, \dots, \Delta b_n]^T \quad (5.64)$$

The faults will be associated with the non-zero elements in this vector. Furthermore, the size of the fault can also be estimated from the magnitudes of the non-zero elements.

In the case of sensor bias, it is said that the parameter estimates converge to a set of biased system parameters, [15], $\hat{\theta} \rightarrow \theta + \theta_b$, where θ_b is the estimation bias. Therefore, faults can still be detected, but the estimated parameter vector can no longer be used for fault isolation.

5.5 Comparison of State Estimation and Parameter Estimation based FDI Schemes

Based on the previous analysis, it is clear that the state estimation and the parameter estimation based FDI schemes share some similarities, but also have significant differences.

For the state estimation based FDI schemes, one can conclude that:

(1) The detection delay is relatively small. Both observers and Kalman filters have exponential rate of convergence. This feature is extremely important to minimize the fault detection delay.

(2) There are less stringent requirements on the system input signal. The requirement on the input for the state estimation based FDI schemes is significantly relaxed. No persistent excitation conditions are needed.

(3) Low fault isolatibility. One of the major deficiencies in all state estimation based FDI approaches is the low fault isolability. There are total of $2n$ parameters which may undergo changes as a result of a fault in the system. However, the fault detection variable is only a scalar. It is impossible for the algorithm to provide either the exact location or the size of the fault.

Therefore, one can conclude that the state estimation based schemes have very small detection delay, and are effective in detecting fast developing faults. However, due to the lack of separation of the individual system parameters when synthesizing the fault detection variables, it is very difficult for the algorithm to isolate the source of the fault, as well as to estimate the size of the fault.

In contrast, the RLS parameter estimation based FDI scheme possess the following properties:

(1) The detection delay is relatively large. The FDI decision can only be made after the parameter estimates converge to their true values. In RLS parameter estimation based FDI schemes, the rate of convergence is only $(1/k)$. Such a convergence rate may be too slow for some applications, which will lead to a large detection delay.

(2) The information on the fault and the post-fault system is available. The location and the size of the fault as well as the effect of the fault on the system can be readily determined from the parameter estimates. Such detailed information is important to the design of reconfigurable control systems.

(3) The requirement on the richness of the input signal is high. The persistent excitation condition of the system input is one of the necessary conditions for the convergence of the parameter estimation algorithm. In many practical situations, this condition may be difficult to satisfy during steady-state operation, which precludes the use of such a method for FDI.

Based on the above analysis, parameter estimation based FDI schemes are extremely powerful in isolating the fault and estimating the fault size. However, they usually have a large detection delay, and one also has to pay particular attention on the richness of the system input signal.

In summary, it becomes very clear that both parameter estimation and state estimation based FDI schemes offer unique strengths and weaknesses. They indeed complement each other in terms of their fault detection speeds, fault isolatability, etc. In active FTCS designs, one may have to use both types of schemes to achieve rapid fault detection as well as detailed fault identification.

5.6 A New FDI Scheme Based on A Bounding Parameter Estimation Algorithm

The critical issue in any active FTCS is the limited amount of time available for the fault detection and identification, and the control system reconfiguration. A large time delay between the instance of the fault occurrence and the onset of the control reconfiguration could result in large fault-induced transients, and even lead to loss of the system stability. In fact, there exists a conflicting requirement between the amount of time that the FDI scheme takes and the amount of information that the FDI scheme provides. This is one of the main difficulties in integrating a FDI scheme with a control reconfiguration strategy effectively. In practice, it is impossible for a FDI scheme to provide the exact information on the post-fault system immediately after the fault occurrence. For example, in the case of parameter estimation based FDI schemes, the time taken for the FDI scheme to obtain the precise post-fault system parameters depends on the convergence rate of the RLS estimation algorithm, which is usually slow as shown in Lemma 5.2.

Therefore, for fast response of the control system reconfiguration, one has to design a fast fault detection scheme that can pick out the fault occurrence promptly and an effective fault identification scheme that can provide the most up-to-date information on the post-fault system right after the detection of the fault. The post fault information provided by the fault identification scheme at the first several steps usually has limited precision, however, instead of waiting for more precise information, the control reconfiguration scheme should be able to immediately incorporate such information and take control actions. Gradually, as more precise information becomes available, and the reconfiguration scheme is updated correspondingly until the system performance is recovered.

It is clear that the concept of “graceful degradation” is reflected in this design philosophy. As illustrated in Chapter 2, the objectives of a fault tolerant control system can be divided into high priority and low priority ones. When faults occur, the most important thing for FTCS is to achieve high priority objectives to protect the system from fatal failure. One measure of these high priority objectives is the allowable space and the hard

deadline (see Section 2.4.4, Chapter 2). By the first-step reconfiguration, the system performance may not be completely recovered, but some critical system states should be maintained within the allowable space. In other words, the hard deadline of the system is extended. This is extremely important for further control actions to recover the pre-fault system performance.

As illustrated in the preceding sections, the state-estimation based fault detection scheme is more appropriate for the task of fast fault detection. In this section, a bounding parameter estimation algorithm [16] is proposed for fault identification. The advantage of this algorithm is that it can provide a sequence of estimated bounds on the post-fault system parameters. The true system parameters are confined within the corresponding bounds which will shrink as parameter estimation algorithm progresses. It is required that the control reconfiguration scheme should be insensitive to the differences between the real post-fault system parameters and the identified ones, i.e the estimation errors. However, such estimation errors are usually unknown. Therefore in this case, the parameter bounds, within which the estimation errors are limited, turn out to be extremely important in designing the control reconfiguration scheme. The estimation bound in this case act as a measure of the precision of the post fault system information from the early fault identification results.

Based on the open-loop system model as described in EQ (5.40) & (5.41), with the assumption that the equation error $\omega(k)$ is a bounded noise term, i.e.

$$|\omega(k)| \leq \eta(k) \quad k \geq 0 \quad (5.65)$$

where $\eta(k)$ is assumed to be known *a priori*.

The system parameters θ will belong to the following parameter set:

$$S(k) = \{ \theta | y(k) - \eta(k) \leq \psi^T(k) \theta \leq y(k) + \eta(k) \} \quad (5.66)$$

where $S(k)$ is so-called a parameter membership set or feasible parameter set. From a geometric viewpoint, this set can be viewed as a polyhedral region in the parametric space which is delimited by pairs of parallel planes (or lines in the two-dimensional case) $\bar{D}(k)$ and $\underline{D}(k)$ produced from the new measurements, i.e.

$$\begin{aligned}\bar{D}(k) &= \{ \theta | \psi^T(k) \theta = y(k) + \eta(k) \} \\ \underline{D}(k) &= \{ \theta | \psi^T(k) \theta = y(k) - \eta(k) \}\end{aligned}\quad (5.67)$$

$S(k)$ is a monotone non-increasing sequence of the set. It is depicted in Figure 5.3 for the two-dimensional case. It is clear that any parameter vector θ within the set $S(k)$ is a valid estimation. Usually, the center of the region is chosen as the estimate of true system parameters.

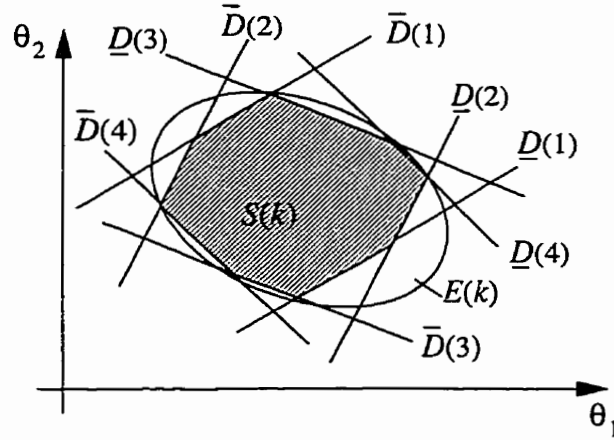


Figure 5.3 The parameter membership set $S(k)$ and its ellipsoid outer bounding approximation

In order to calculate the central estimate, one has to determine the membership set $S(k)$. However, it is difficult to solve this problem since the number of measurements increases linearly in k , and it involves solving $2k$ n -th order inequalities in EQ (5.66). However, by approximating this irregular shaped convex region using an ellipsoid shaped region, $E(k)$, the computational aspect of this problem can be simplified. The algorithm is

called the ellipsoidal outer bounding algorithm, and was first introduced by Fogel and Huang, [17]. In this algorithm, the $E(k)$ is chosen to enclose $S(k)$ as “tightly” as possible. A recursive version of this scheme is employed here.

For the system equation given in EQ (5.41), an ellipsoid $E(k)$ is chosen as the following form:

$$E(k) = \{ \theta | [\theta - \hat{\theta}(k)]^T P^{-1}(k) [\theta - \hat{\theta}(k)] \leq \sigma^2(k) \} \quad (5.68)$$

where $\sigma^2(k)$ is the upper bound of the ellipsoid $E(k)$. The initial value $E(0)$ is chosen as:

$$E(0) = \{ \theta | [\theta - \theta(0)]^T P^{-1}(0) [\theta - \theta(0)] \leq \sigma_0^2 \} \quad (5.69)$$

where $\sigma_0^2 = \sigma^2(0)$.

The covariance matrix $P(k)$ is calculated based on the following equation:

$$P(k) = \frac{1}{\alpha(k)} \left[P(k-1) - \frac{\beta(k) P(k-1) \psi(k) \psi^T(k) P(k-1)}{\alpha(k) + \beta(k) \psi^T(k) P(k-1) \psi(k)} \right] \quad (5.70)$$

where $\alpha(k)$ and $\beta(k)$ are the forgetting and the selecting factors, respectively, and the initial value $P(0)$ is chosen as:

$$P(0) = I_{2n} / (\epsilon \sigma_0^2) \quad (5.71)$$

ϵ is a sufficiently small positive number such that $E(0)$ contains $S(k)$ for all $k \geq 0$, I_{2n} is the identity matrix of order $2n$.

The estimated parameters are calculated as follows and they correspond to the center of the ellipsoid defined in EQ (5.68):

$$\hat{\theta}(k) = \hat{\theta}(k-1) + \beta(k) P(k-1) \psi(k) [y(k) - \psi^T(k) \hat{\theta}(k-1)] \quad (5.72)$$

The ellipsoid upper bound $\sigma^2(k)$ is updated using the following equation:

$$\sigma^2(k) = \alpha(k) \sigma^2(k-1) + \beta(k) \eta^2(k) - \frac{\alpha(k) \beta(k) [y(k) - \psi^T(k) \hat{\theta}(k-1)]^2}{\alpha(k) + \beta(k) \psi^T(k) P(k-1) \psi(k)} \quad (5.73)$$

In order to ensure the smallest ellipsoid that enclose $S(k)$, $\sigma^2(k)$ can be minimized by choosing proper $\beta(k)$ (fixing $\alpha(k) = \alpha$). From EQ (5.73), by minimizing $\sigma^2(k)$ with respect to $\beta(k)$, $\beta^*(k)$ can be calculated as follows:

$$\beta^*(k) = \frac{\alpha}{\psi^T(k) P(k-1) \psi(k)} \left(\frac{|y(k) - \psi^T(k) \hat{\theta}(k-1)|}{\eta(k)} - 1 \right) \quad (5.74)$$

Therefore, at every instant k , $\beta(k)$ is chosen as:

$$\beta(k) = \begin{cases} 0 & \text{if } |y(k) - \psi^T(k) \hat{\theta}(k-1)| \leq \eta(k) \quad \text{or} \quad \psi^T(k) P(k-1) \psi(k) = 0 \\ \beta^*(k) & \text{otherwise} \end{cases} \quad (5.75)$$

Lemma 5.3: *The ellipsoid upper bound $\sigma^2(k)$ is a monotone decreasing sequence, by choosing $\alpha(k) = \alpha$, $0 < \alpha < 1$ and $\beta(k)$ as in EQ (5.75).*

Proof:

By defining:

$$\Omega(k) = \psi^T(k) P(k-1) \psi(k) \quad (5.76)$$

$$\varepsilon(k) = y(k) - \psi^T(k) \hat{\theta}(k-1) \quad (5.77)$$

EQ (5.73) can be written as:

$$\sigma^2(k) = \alpha \sigma^2(k-1) + \beta(k) \eta^2(k) - \frac{\alpha \beta(k) \varepsilon^2(k)}{\alpha + \beta(k) \Omega(k)} \quad (5.78)$$

Since $\beta(k)$ is chosen to minimize $\sigma^2(k)$, i.e. $\frac{\partial}{\partial \beta(k)} \sigma^2(k) = 0$, which gives:

$$\eta^2(k) = \frac{\alpha^2 \varepsilon^2(k)}{[\alpha + \beta(k) \Omega(k)]^2} \quad (5.79)$$

Substitute EQ (5.79) into EQ (5.78), and by simple manipulation, the following equation can be obtained:

$$\sigma^2(k) = \alpha \sigma^2(k-1) - \frac{\alpha \beta^2(k) \varepsilon^2(k) \Omega(k)}{[\alpha + \beta(k) \Omega(k)]^2} \quad (5.80)$$

From EQ (5.75), when $\beta(k) = 0$, the above equation becomes:

$$\sigma^2(k) = \alpha \sigma^2(k-1) \quad (5.81)$$

Therefore, if choosing $0 < \alpha < 1$, $\sigma^2(k)$ is a monotone decreasing.

When $\beta(k) = \beta^*(k)$ as shown in EQ (5.74), i.e.

$$\beta(k) = \beta^*(k) = \frac{\alpha}{\Omega(k)} \left(\frac{|\varepsilon(k)|}{\eta(k)} - 1 \right) \quad (5.82)$$

EQ (5.80) becomes:

$$\sigma^2(k) = \alpha \sigma^2(k-1) - \frac{\alpha \varepsilon^2(k)}{\Omega(k)} \cdot \frac{\gamma^2(k)}{(1 + \gamma(k))^2} \quad (5.83)$$

where $\gamma(k) = \frac{|\varepsilon(k)|}{\eta(k)} - 1$. Since the second term of the above equation is greater than or equal to zero, one can obtain that

$$\sigma^2(k) \leq \alpha \sigma^2(k-1) \quad (5.84)$$

By choosing $0 < \alpha < 1$, $\sigma^2(k)$ is monotone decreasing.

Therefore, the ellipsoid upper bound $\sigma^2(k)$ is a monotone decreasing sequence, by choosing $\alpha(k) = \alpha$, $0 < \alpha < 1$ and $\beta(k)$ as in EQ (5.75). $\square$

From EQ (5.68), the upper and lower bounds of the estimated parameters from the above algorithm can be calculated, and the true parameters lie in these bounds:

$$\hat{\theta}_{i,min}(k) \leq \theta_i^* \leq \hat{\theta}_{i,max}(k) \quad (5.85)$$

where

$$\begin{aligned} \hat{\theta}_{i,min}(k) &= \hat{\theta}_i(k) - \sigma(k-1) [P_{(i,i)}(k)]^{1/2} \\ \hat{\theta}_{i,max}(k) &= \hat{\theta}_i(k) + \sigma(k-1) [P_{(i,i)}(k)]^{1/2} \end{aligned} \quad (5.86)$$

therefore

$$-\sigma(k-1) [P_{(i,i)}(k)]^{1/2} \leq \theta_i^* - \hat{\theta}_i(k) \leq \sigma(k-1) [P_{(i,i)}(k)]^{1/2} \quad (5.87)$$

where $\hat{\theta}_{i,max}(k)$ and $\hat{\theta}_{i,min}(k)$ denote maximum and minimum values taken by $\hat{\theta}_i(k)$, the i th element of $\hat{\theta}(k)$. Since $\sigma(k)$ is a monotonically decreasing sequence, which means that the size of $E(k)$ is decreasing, therefore, the size of estimation error bounds defined in EQ (5.87) is decreasing too.

From EQ (5.68), it is clear that $\sigma^2(k)$ is also the upper bound of the following quadratic function:

$$V(k) = [\theta^* - \hat{\theta}(k)]^T P^{-1}(k) [\theta^* - \hat{\theta}(k)] \quad (5.88)$$

The study of the convergence properties of the above algorithm can then be carried out and the results are given in the following lemma, [16]:

Lemma 5.3: *If the following persistent excitation condition on the input signal is satisfied:*

$$mI_n \leq \sum_{i=k}^{k+N} \beta(i) \psi(i) \psi^T(i) \leq MI_n \quad (5.89)$$

where m, M and N ($N \geq n$) are positive scalars.

Then, there exists a $\rho > 0$ so that $P^{-1}(k) \geq \rho I_{2n} > 0$, and

$$(1) \lim_{k \rightarrow \infty} \|\theta(k) - \theta(k-1)\|^2 = 0;$$

$$(2) \|\tilde{\theta}(k)\|^2 \leq \frac{\varepsilon \sigma_0^2}{\rho} \cdot \alpha^k \cdot \|\tilde{\theta}(0)\|^2 \quad \forall k \geq N+1;$$

$$(3) \|\tilde{\theta}(k)\|^2 \leq \frac{1}{\rho} \cdot \sigma^2(k)$$

where $\tilde{\theta}(k) = \theta^* - \hat{\theta}(k)$; ε and σ_0 are scalars chosen in EQ (5.71).

Therefore, it can be seen from property (2) of the above lemma, the bounding parameter estimation algorithm has an exponential rate of convergence. From property (3), the square of the steady-state estimation error has an upper bound, $\sigma^2(\infty)/\rho$.

It should be emphasized that the parameter estimates are not updated at every step. As can be seen from EQ (5.75), a dead zone is used in the calculation of the forget-

ting factor $\beta(k)$ so that the redundant data can be discarded. In other words, the estimated parameters, as well as their bounds, do not change for the time instances corresponding to $\beta(k) = 0$. In fact, the estimated parameters and their bounds only be updated in a step-wise fashion. For this reason, a new time variable h is introduced to represent the consecutive steps at which the estimates are updated. This time variable can be calculated as follows:

$$\begin{aligned} k &= k+1 \\ \text{if } \beta(k) &= 0 \text{ then } h = h \\ \text{else } h &= h+1 \end{aligned} \tag{5.90}$$

By replacing k with h , the estimated parameter vector and the parameter bounds depicted in EQ (5.72) and EQ (5.86) can be written as $\hat{\theta}(h)$, $\hat{\theta}_{min}(h)$ and $\hat{\theta}_{max}(h)$ respectively. It will be demonstrated later in Chapter 6 that h can help integrate the post-fault system identification scheme with the reconfigurable control.

It is required that the control reconfiguration be prompt and effective in order to maintain the high priority system performance when the fault occurs, especially in the most critical period of active FTCS, i.e. during the fault (see Figure 2.6 in Chapter 2). However, the speed and the effectiveness of the reconfigurable control system depend greatly on the FDI scheme. For the above described fault identification scheme, at the moment right after the fault occurrence, the estimation error bounds are usually large, which makes the design of reconfigurable control more difficult. The difficulty lies in the fact that the control should be able to accommodate the estimation error caused by such an imprecise fault identification. More details on designing a reconfigurable control system that can be integrated with the proposed FDI scheme will be discussed in Chapter 6: *Design of Reconfigurable Control Systems*.

5.7 Conclusion

In this chapter, design issues of Fault Detection and Identification schemes are discussed. Two common design techniques based on state estimation and parameter estimation are introduced and compared. The important issue of integration of FDI with the reconfigurable control system is addressed. Finally, a new FDI scheme is proposed using the fast state-estimation based fault detection scheme and a bounding parameter estimation based fault identification scheme.

5.8 Bibliography

- [1] J. C. Deckert, M. N. Desai, J. J. Deyst and A. S. Willsky, "F-8 DFBW sensor failure identification using analytical redundancy," *IEEE Trans. Automatic Control*, AC-22 (5), pp. 795-803, 1977.
- [2] H. Wang and S. Daley, "A fault detection method for unknown systems with unknown input and its application to hydraulic turbine monitoring," *International Journal of Control*, vol. 57, no. 2, pp. 247-260, 1993.
- [3] W. C. Merrill, "Sensor failure detection for jet engines using analytical redundancy," *Journal of Guidance, Control & Dynamics*, vol. 8, no 6, pp. 673-682, 1985.
- [4] R. J. Patton and J. Chen, "A review of parity space approaches to fault diagnosis for aerospace systems," *Journal of Guidance, Control & Dynamics*, vol. 17, no. 2, pp. 278-285, 1994.
- [5] J. Gertler and G. DiPierro, "On the relationship between parity relations and parameter estimation," *Pre-prints of IFAC Symposium SAFEPROCESS'97*, pp. 468-473, 1997.
- [6] F. Jia and J. Jiang, "Fault diagnosis in DC servo systems: a comparative study of three fault diagnosis schemes," *European Journal of Diagnosis and Safety in Automation*, vol. 4, no. 4, pp.357-374, 1994.

- [7] P.M. Frank, "Analytical and qualitative model based fault diagnosis - a survey and some new results," *European Journal of Control*, vol. 2, pp. 6-28, 1996.
- [8] E. A. Garcia and P. M. Frank, "On the relationship between observer and parameter identification based approaches to fault detection," *Pre-prints of the 13th IFAC World Congress*, pp. 25-30, 1996.
- [9] D. Van Schrick, "FDI residual generators - a comparison," *Preprints of IFAC Symposium, SAFEPROCESS'94*, pp. 545-550, 1994.
- [10] G. C. Goodwin and K. S. Sin, *Adaptive Filtering Prediction and Control*, Prentice Hall, Englewood Cliffs, NJ, 1984.
- [11] B. D. O. Anderson and J. B. Moore, *Optimal Filtering*, Prentice Hall, Englewood Cliffs, NJ, 1979.
- [12] E. L. Lehmann, *Testing Statistical Hypotheses*, 2nd ed. Wiley, NY, 1986.
- [13] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*, Prentice Hall, Englewood Cliffs, NJ, 1993.
- [14] R. Patton, P. Frank and R. Clark, *Fault Diagnosis in Dynamic Systems, Theory and Application*, edited, Prentice Hall Ltd., UK, 1989.
- [15] L. Ljung, *System Identification: Theory for the User*, Prentice Hall, Englewood Cliffs. NJ, 1987.
- [16] M. Milanese, J. Norton, H. Piet-Lahanier and E. Walter, *Bounding Approaches to System Identification*, Plenum Press, New York, 1996.
- [17] E. Fogel and Y. F. Huang, "On the value of information in the system identification-bounded noise case," *Automatica*, Vol. 18, No. 2, pp. 229-238, 1992.

Design of Reconfigurable Control Systems

6.1 Introduction

In contrast with passive FTCS, active FTCS react to the system component failures actively by reconfiguring control laws so that the stability/performance of the entire system can be maintained. To achieve a successful control reconfiguration, such a system relies on a real-time fault detection and identification scheme to provide the most up-to-date information about the post-fault system.

There are a lot of techniques already available for reconfigurable control, such as the pseudo-inverse method, [1]; model following methods, [2]; and eigenstructure assignment methods, [3], etc. However, almost all of these methods are based on the assumption that a perfect post-fault information is already available, which is seldom the case in practice. As mentioned in Chapter 5, it is impossible for a FDI scheme to provide the exact information on the post-fault system immediately after the fault occurrence.

Since active FTCS involve a significant amount of on-line fault detection, real-time decision-making and control, the system timing is extremely important. As illustrated in Chapter 2, the performance of active FTCS in the duration of faults depends very much on the speed of FDI and reconfigurable control. Generally speaking, in the presence of

† : A version of this chapter has been prepared for submission to *Automatica, the Journal of IFAC*:

Q. Zhao and J. Jiang, "Reconfigurable control design based on a bounding parameter estimation scheme."

faults/failures, it is required that the reconfigurable control action be taken as promptly as possible. On the other hand, the correctness of the control action is another important aspect, which depends heavily on up-to-date information on the fault, which is provided by FDI. Therefore, the trade-off between the speed and the correctness of the reconfigurable control, and the interaction between reconfigurable control and the FDI scheme are two major important issues in active FTCS. Furthermore, the trade-off between the stability and the performance of the overall system should also be carefully considered.

The faults considered in this chapter are assumed to be the system dynamic faults which has been defined and modelled in Section 2.1. Some of the existing design methods for reconfigurable control are briefly reviewed. A new active FTCS design methodology will then be introduced, where the FDI scheme and the reconfigurable system are integrated. In this method, the bounding parameter estimation algorithm described in Chapter 5 will be utilized to provide post-fault information with a set of parameter bounds. A robust controller can be immediately synthesized to start stabilizing the system without waiting for the final convergence of the fault identification scheme. As more data becomes available, the fault information will become more precise (since parameter bounds become tighter), and the control system performance will be improved gradually.

6.2 Review of Existing Design Techniques for Reconfigurable Control Systems

6.2.1 Pseudo-inverse method

The Pseudo-Inverse Method (PIM) is a well-known method in reconfigurable control and has been applied to practical systems, such as flight control systems, [4]. The idea behind the PIM is to make the closed-loop system matrix of the reconfigurable system as close as possible to that of the nominal system. One of the advantages of this method is its simplicity in calculating the reconfigurable control law. However, there is an assumption in this method that perfect information on post-fault system is available. In

other words, such a method is only for the controller redesign based on known failure information.

Let the nominal open-loop system be given in EQ (2.1). A state feedback control can be used:

$$u(t) = Kx(t) \quad (6.1)$$

where $K \in \mathbb{R}^{m \times n}$ is the feedback gain matrix.

When the system dynamic faults have occurred, the post-fault system model becomes EQ (2.10) as described in Chapter 2, which is rewritten as,

$$\dot{x}(t) = A_f x(t) + B_f u(t) \quad (6.2)$$

where $A_f = A + \Delta A$, $B_f = B + \Delta B$.

Therefore, in order to recover the nominal system performance, it is highly desirable that the reconfigured closed-loop system matrix after reconfiguration be the same as that of the nominal system, i.e.

$$A_f + B_f K_r = A + BK \quad (6.3)$$

where $K_r \in \mathbb{R}^{m \times n}$ is the new state-feedback gain. By assuming A_f and B_f are known, K_r can be calculated from EQ (6.3). However, in most cases, B_f is not invertible. Therefore K_r can only be obtained such that the closed-loop system matrix $A_f + B_f K_r$ approximates to the nominal one $A + BK$. The approximation solution is given by:

$$K_r = B_f^\dagger (A - A_f + BK) \quad (6.4)$$

where $B_f^\dagger$ is the pseudo-inverse of B_f .

A pseudo-inverse is defined in [5]. If the matrix $N \in \mathfrak{R}^{n \times m}$ has r non-zero singular values $\sigma_i, i = 1, \dots, r$, then it has a singular value decomposition of the following form:

$$N = U \cdot \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix}_{n \times m} \cdot V^H \quad (6.5)$$

where $S = \text{diag} \{ \sigma_i \}, \forall i = 1, \dots, r$, $U \in \mathfrak{R}^{n \times n}$ and $V \in \mathfrak{R}^{m \times m}$ are unitary matrices. The decomposition has the following properties:

$$\begin{aligned} U^H U &= U U^H, V^H V = V V^H = I \\ |\lambda_i[U]|^2 &= 1, |\lambda_i[V]|^2 = 1 \end{aligned} \quad (6.6)$$

where $(\cdot)^H$ denotes the conjugate transpose.

The pseudo-inverse of N is then defined as:

$$N^\dagger = V \begin{bmatrix} S^{-1} & 0 \\ 0 & 0 \end{bmatrix}_{m \times n} U^H \quad (6.7)$$

Based on the above definition, K_r can then be calculated as shown in EQ (6.4). By using such a reconfigurable state feedback control, it is known that the following norm is minimized:

$$J = \| (A_f + B_f K_r) - (A + B K) \|_F \quad (6.8)$$

where $\| \cdot \|_F$ denotes the Frobenius norm, which is defined as:

$$\text{for } A = [a_{i,j}] \in \mathbb{R}^{n \times n}, \|A\|_F = \left(\sum_{i,j=1}^n |a_{i,j}|^2 \right)^{\frac{1}{2}} \quad (6.9)$$

Therefore, by the control reconfiguration, the closed-loop faulty system matrix approximates to the nominal one, in the sense that the Frobenius norm of the difference of two matrices is minimized. For the system stability, it has been shown that the reconfigured closed-loop system is stable only when the nominal system eigenvalues are located relatively far left of imaginary axis and the norm in EQ (6.8) is sufficiently small, [1]. However, these conditions are rather restrictive in the context of a fault tolerant control system. In the event that these conditions are not satisfied, it is possible to have an unstable system by using the PIM. In other words, this method cannot guarantee the system stability.

Recognizing the lack of a stability guarantee when using the PIM, a modified PIM (MPIM) has been proposed in [6]. MPIM makes use of results on stability robustness of linear systems with structured uncertainties. By restraining the reconfigured feedback gain K_r in a stability bound, the control design problem is formulated as a constrained minimization problem. Although the stability can be guaranteed using MPIM, the stability bound is always too restrictive to be of any practical use. This method only works well with mild system component faults/failures.

6.2.2 Model-following method

For PIM and MPIM, the design idea is to make the closed-loop system matrix of the reconfigured system close to that of the nominal system. An alternative design method called the model following method (MFM), shares a similar design philosophy. The only difference between the MFM and the PIM is the measure of such closeness and the technique used to minimize it. The design objective of the model following method is

to make the state trajectories of the reconfigured system as close to those of the nominal system as possible.

Based on the impaired system shown in EQ (6.2), let the reference model be:

$$\dot{x}_m(t) = A_m x_m(t) + B_m u_m(t) \quad (6.10)$$

where the order of above model is assumed to be as same as that in EQ (6.2). Therefore, $\{A_m, B_m, C_m\}$, $x_m(t)$, $u_m(t)$ and $y_m(t)$ are of same dimensions with those in EQ (6.2), respectively. It is assumed that the input of the reference model, u_m , is piecewise continuous.

By assuming that the reference model $\{A_m, B_m, C_m\}$ is known explicitly, the structure of the reconfigurable system is depicted in Figure 6.1.

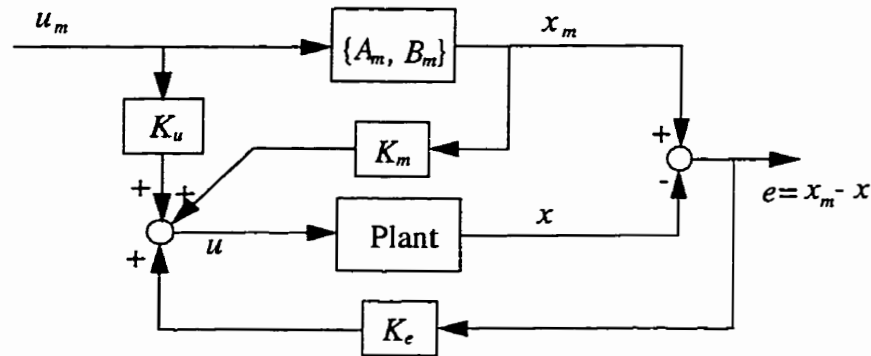


Figure 6.1 Control system structure using explicit model-following method, [6].

It is clear that the reference model is implemented as part of the control system. K_e is the stabilizing gain. The control input of the system is

$$u(t) = K_e e(t) + [K_m x_m(t) + K_u u_m(t)] \quad (6.11)$$

From EQ (6.2) and EQ (6.10), the state error can be obtained,

$$\dot{e}(t) = A_f e(t) + (A_m - A_f) x_m(t) + B_m u_m(t) - B_f u(t) \quad (6.12)$$

By substituting EQ (6.11) into EQ (6.12), the error can be rewritten as:

$$\begin{aligned} \dot{e}(t) &= (A_f - B_f K_e) e(t) + \{ (A_m - A_f) x_m(t) + B_m u_m(t) - B_f [K_m x_m(t) + K_u u_m(t)] \} \\ &= (A_f - B_f K_e) e(t) + d(t) \end{aligned} \quad (6.13)$$

where $d(t) = (A_m - A_f) x_m(t) + B_m u_m(t) - B_f [K_m x_m(t) + K_u u_m(t)]$.

One can choose K_m and K_u as follows:

$$\begin{aligned} K_m &= B_f^\dagger (A_m - A_f) \\ K_u &= B_f^\dagger B_m \end{aligned} \quad (6.14)$$

so that the l_2 norm of $d(t)$ is minimized:

$$\begin{aligned} \min J_m &= \min \|\dot{e} - (A_f - B_f K_e) e\|_2 \\ &= \min \|(A_m - A_f) x_m + B_m u_m - B_f [K_m x_m + K_u u_m]\|_2 \end{aligned} \quad (6.15)$$

It should be pointed out that, under certain conditions, $d(t)$ can be equal to zero. This is shown as below:

With the above control gains K_m and K_u , EQ (6.13) can be rewritten as:

$$\dot{e}(t) = (A_f - B_f K_e) e(t) + (I - B_f B_f^\dagger) (A_m - A_f) x_m(t) + (I - B_f B_f^\dagger) B_m u_m(t) \quad (6.16)$$

Therefore, if the following conditions are satisfied

$$\begin{cases} (I - B_f B_f^\dagger) (A_m - A_f) = 0 \\ (I - B_f B_f^\dagger) B_m = 0 \end{cases} \quad (6.17)$$

then $d(t) = 0$, and the equation of the state error becomes:

$$\dot{e}(t) = (A_f - B_f K_e) e(t) \quad (6.18)$$

The conditions in EQ (6.17) are known as Erzberger's conditions, [7]. From EQ (6.18), it is clear that if the post-fault system is stabilizable, one can design the stabilizing control gain K_e , so that the eigenvalues of the above error equation are assigned to the left half s -plane, and therefore,

$$e(t) \rightarrow 0 \text{ or } x(t) \rightarrow x_m(t) \text{ as } t \rightarrow \infty \quad (6.19)$$

It can be seen that Erzberger's conditions are sufficient conditions for achieving the state trajectory tracking. More often than not, $d(t) \neq 0$, and:

$$\dot{e}(t) = (A_f - B_f K_e) e(t) + d(t) \quad (6.20)$$

where

$$d(t) = (I - B_f B_f^\dagger) (A_m - A_f) x_m(t) + (I - B_f B_f^\dagger) B_m u_m(t) \neq 0 \quad (6.21)$$

In this case, the states of the reconfigured system will no longer follow the reference model states, however, the distance between the two state trajectories (i.e. the error $e(t)$) will be bounded. This is because EQ (6.20) will be bounded-input and bounded-output stable as long as the reference model is stable and the input u_m is bounded, [6]. Therefore, the stability of the reconfigured system can be guaranteed by using the perfect model following method.

One of the disadvantages of the above method is the difficulty in choosing the reference model for the reconfigured system. A proper reference model should be chosen such that it not only has the desired performance, but also is relatively 'easy' for the reconfigured system to follow its state trajectories closely. From EQ (6.21), although the l_2 norm of $d(t)$ is minimized by choosing K_m and K_u as in EQ (6.14), it can still be rather large for some choices of the reference model $\{A_m, B_m\}$. The value of $d(t)$ also depends on different failure modes, $\{A_f, B_f\}$. Therefore, the distance between the state trajectories of the reference model and the reconfigured system can be large with an inappropriate combination of the reference model and under some failure cases.

6.2.3 Eigenstructure assignment method

From the viewpoint of stability and performance recovery, the reconfigurable control can also be designed to recover the system eigenvalues, and the eigenvectors. This design philosophy has been realized in [3], where an eigenstructure assignment based reconfigurable control design method is proposed. This method not only guarantees the stability of the reconfigured system by recovering the system eigenvalues, but also recovers the system performance to the maximum extent by placing the eigenvectors as close to those of the original system as possible.

As in the previous case, the nominal open-loop system is given EQ (2.1), and a state feedback control is used. The closed-loop system can be written as:

$$\dot{x}(t) = (A + BK_o)x(t) \quad (6.22)$$

where $K_o \in \mathbb{R}^{m \times n}$ is the state-feedback gain matrix of the nominal system $\{A, B\}$.

For the above system, it is well known that there exists a solution of state feedback gain, K , such that: (1) n self-conjugate eigenvalues can be arbitrarily assigned; (2)

m entries in each eigenvector of a total n of eigenvectors can be arbitrarily assigned; and (3) the achievable eigenvectors must lie in the subspace spanned by $\{(\lambda_i I - A)^{-1} B, i = 1, 2, \dots, n\}$, where λ_i is the i th eigenvalue of the closed-loop system, [8].

When a fault occurs in the system, the system model becomes EQ (6.2). Based on this model, a new state-feedback control law needs to be synthesized in order to stabilize the post-fault system. The closed-loop system then becomes:

$$\dot{x}(t) = (A_f + B_f K_f) x(t) \quad (6.23)$$

where $K_f \in \mathbb{R}^{m \times n}$ is the reconfigured state-feedback gain matrix. In this case, K_f can be designed to place the eigenvalues of the post-fault close-loop system at the desired locations, which can be chosen to be the same as those of the original nominal system, i.e.

$$\lambda \{A_f + B_f K_f\} = \{\lambda_i, i = 1, 2, \dots, n\} = \lambda \{A + B K_o\} \quad (6.24)$$

For multivariable systems, the solution of K_f satisfying the above equation is not unique. In addition, one can choose K_f such that the eigenvectors of the reconfigured system are as close to those of the nominal system as possible.

Since,

$$(A_f + B_f K_f) v_i^f = \lambda_i v_i^f \quad (6.25)$$

where v_i^f is the i th closed-loop eigenvector of the reconfigured system. From this equation, it can be obtained that

$$v_i^f = (\lambda_i I - A_f)^{-1} B_f K_f v_i^f \quad (6.26)$$

By denoting $S_i = (\lambda_i I - A_f)^{-1} B_f$, $S_i \in \mathbb{R}^{n \times m}$, and $g_i = K_f v_i^f$, $g_i \in \mathbb{R}^{m \times 1}$,

EQ (6.26) becomes

$$v_i^f = S_i \cdot g_i \quad (6.27)$$

Therefore, v_i^f lies in the subspace spanned by S_i . The optimal choice of v_i^f is the orthogonal projection of the corresponding nominal closed-loop system eigenvector, v_i , on S_i , i.e.

$$v_i^f = S_i (S_i^T S_i)^{-1} S_i^T v_i \quad (6.28)$$

The above choice of v_i^f will minimize the l_2 norm of the difference between v_i and v_i^f :

$$\text{Min } (v_i - v_i^f)^T (v_i - v_i^f) \quad (6.29)$$

where v_i is the i th desired eigenvector of the nominal system.

Now the problem is how to calculate K_f to achieve the above v_i^f . In order to solve this problem, a linear transformation $T = [B_f P] \in \mathbb{R}^{n \times n}$ is applied to the post-fault system, one can have

$$\underline{A}_f := T^{-1} A_f T, \quad \underline{B}_f := T^{-1} B_f = \begin{bmatrix} I_m \\ 0_{(n-m) \times m} \end{bmatrix} \quad (6.30)$$

$$\underline{v}_i^f := T^{-1} v_i^f \quad (6.31)$$

and

$$\left(\underline{A}_f + \underline{B}_f K_f \right) \underline{v}_i^f = \lambda_i \underline{v}_i^f \quad (6.32)$$

By partitioning $\underline{A}_f$ and $\underline{v}_i^f$ according to the partition of $\underline{B}_f$:

$$\underline{A}_f = \begin{bmatrix} \underline{A}_{11} & \underline{A}_{12} \\ \underline{A}_{21} & \underline{A}_{22} \end{bmatrix} = \begin{bmatrix} \underline{A}_1 \\ \underline{A}_2 \end{bmatrix} \quad \underline{v}_i^f = \begin{bmatrix} w_i \\ q_i \end{bmatrix} \quad (6.33)$$

where $\underline{A}_1 = \begin{bmatrix} \underline{A}_{11} & \underline{A}_{12} \end{bmatrix}$ and $\underline{A}_2 = \begin{bmatrix} \underline{A}_{21} & \underline{A}_{22} \end{bmatrix}$.

It can be obtained from EQ (6.32) and EQ (6.33) that

$$K_f \begin{bmatrix} w_i \\ q_i \end{bmatrix} = \lambda_i I_m w_i - \underline{A}_1 \begin{bmatrix} w_i \\ q_i \end{bmatrix} \quad (6.34)$$

or

$$\left(\underline{A}_1 + K_f \right) \underline{v}_i^f = \lambda_i I_m w_i \quad (6.35)$$

$i = 1, 2, \dots, n$

Defining $\underline{V}_f = \begin{bmatrix} \underline{v}_1^f & \underline{v}_2^f & \dots & \underline{v}_n^f \end{bmatrix}$ and $W = \begin{bmatrix} \lambda_1 w_1 & \lambda_2 w_2 & \dots & \lambda_n w_n \end{bmatrix}$, K_f is written as

ten as

$$K_f = \left(W - \underline{A}_1 \underline{V}_f \right) \underline{V}_f^{-1} \quad (6.36)$$

Therefore, a reconfigurable state feedback control is synthesized, which not only assigns all eigenvalues of the reconfigured system to those of the nominal system, but also makes the eigenvectors of the reconfigured system as close to those of the nominal system as possible. It is clear that the main advantage of this method over the PIM and the

model following method is that it can guarantee the complete recovery of the system stability and partially recovery of the system performance. However, this method also requires that the post-fault system information is known or provided by a perfect FDI scheme.

6.3 Design of an Integrated FDI and Reconfigurable Control Scheme

6.3.1 Problem formulation

So far, some existing design techniques for reconfigurable control have been briefly reviewed in the preceding section. All of these methods are based on an assumption that the information about the post-fault system is known *a priori*, or provided by a FDI scheme. Under this assumption, the design problem of reconfigurable control becomes to redesign the controller so that the reconfigured system is close to the nominal system, in terms of their closed-loop system matrices, or their system eigenstructures. Recalling the three time periods in active FTCS, which are described in Chapter 2, it is clear that the above described reconfigurable control design techniques are only suitable for the design in the post-fault period. As illustrated in Chapter 2, the system behavior during the fault is extremely important. If the fault is not appropriately restrained during its development, serious consequences can occur, i.e. the complete breakdown. Therefore, the reconfigurable control design during the fault period needs to be carefully considered, which is closely related to the on-line FDI scheme. The critical timing issue is one of the main concerns during this period.

In Figure 6.2, the structure of a general active FTCS system is illustrated. An on-line FDI scheme is used to provide up-to-date fault information to the reconfigurable control module, and this reconfigurable control module should be able to incorporate such information and update the control parameters accordingly, so that the closed-loop system performance can be maintained without serious degradation. The whole operation of the active FTCS is real-time in nature.

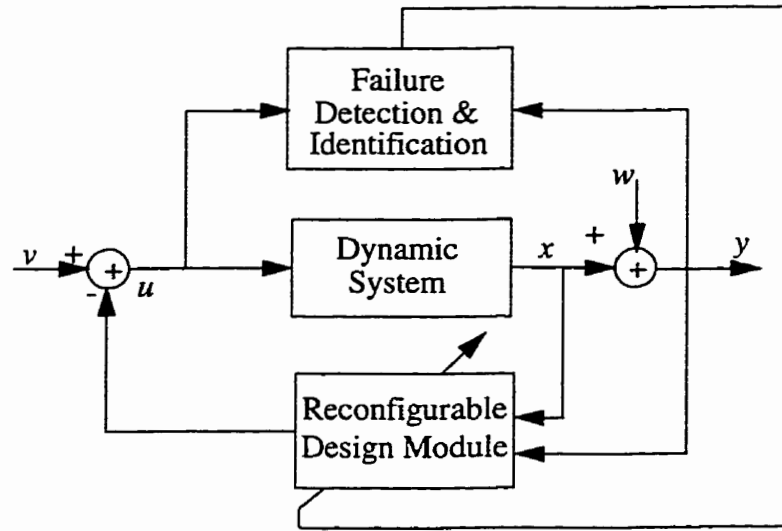


Figure 6.2 A general structure of a reconfigurable control system

In this section, the design issue of the reconfigurable control and its integration with a FDI scheme are investigated. In order to integrate the FDI scheme with the reconfigurable control system, their design should be considered in the same framework, starting right from the system modelling stage. Because FDI schemes are usually in discrete-time form, the system model considered in this section is also in discrete-time form, as was the model in Chapter 5.

Consider a linear discrete-time SISO system in the following state-space representation under nominal operating conditions (no faults):

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) + v(k) \end{aligned} \quad (6.37)$$

where $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times 1}$, and $C \in \mathbb{R}^{1 \times n}$, and $x(t)$, $u(t)$ and $y(t)$ are of appropriate dimensions, respectively. $v(k)$ is the measurement noise, which is assumed to have a white Gaussian distribution with zero mean and a known variance: σ^2 .

With the assumption that only the plant dynamic fault is considered, when such a fault has occurred, the post-fault system state equation becomes:

$$\begin{aligned} x(k+1) &= A_f x(k) + Bu(k) & k \geq k_f \\ A_f &= (A + \Delta A) \end{aligned} \quad (6.38)$$

where ΔA contains the fault-induced changes in the system matrix, and k_f is the time instance of the fault occurrence. The above equation can be written as the following canonical form:

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -a_n & -a_{n-1} & \dots & \dots & -a_1 \end{bmatrix} \quad k < k_f \quad (6.39)$$

$$A_f = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -a_{fn} & -a_{f(n-1)} & \dots & \dots & -a_{f1} \end{bmatrix} \quad k \geq k_f \quad (6.40)$$

$$a_{fi} = a_i + \Delta a_i \quad i = 1, 2, \dots, n \quad (6.41)$$

and

$$\begin{aligned} B &= [0 \ 0 \ \dots \ 1]^T \\ C &= [b_n \ b_{n-1} \ \dots \ b_1] \end{aligned} \quad (6.42)$$

where a_{fi} , $i = 1, 2, \dots, n$, denotes the post-fault system parameters. It needs to be pointed that the parameters in the above canonical state-space representation are identical to those in EQ (5.41) and EQ (5.59), [9].

In Section 5.5, a bounding parameter estimation algorithm based fault identification scheme is proposed. The advantage of this scheme is that it can provide a sequence of estimated bounds on the post-fault system parameters.

$$\hat{\theta}_{i, \min}(k) \leq \theta^*_i \leq \hat{\theta}_{i, \max}(k) \quad (6.43)$$

where θ^*_i is the i th element in the true system parameter vector θ^* , and

$$\theta^* = \begin{cases} \theta & k < k_f \\ \theta + \Delta\theta & k \geq k_f \end{cases} \quad (6.44)$$

$\hat{\theta}_{i, \min}(k)$ and $\hat{\theta}_{i, \max}(k)$ are the estimation bounds, which are calculated in EQ (5.76).

$$\Delta\theta = [\Delta a_1 \ \Delta a_2 \ \dots \ \Delta a_n \ 0 \ \dots \ 0].$$

It should be mentioned that such estimation bounds carry crucial information on the post-fault system parameters. During the critical period of fault occurrence, the control reconfiguration will be synthesized based on these bounds without waiting for the final convergence of parameter estimates. The critical system states can be maintained in the allowable space, and the system stability is retained. When more accurate estimates become available, the reconfiguration control law should be able to refine itself and gradually recover the system performance. The key point of this design philosophy is to extend the system hard deadline at the moment of fault occurrence by a fast control reconfiguration, so that more time can be gained for improving the system performance by subsequent reconfiguration actions.

6.3.2 Design of state-feedback control reconfiguration

1. State-space method based on eigenvalue assignment technique

Since, in the bounding parameter estimation algorithm, the estimated parameters and their bounds only change in a step-wise fashion, the estimated system model becomes a piecewise time-invariant model. It can be written in the following state-space representation:

$$\begin{aligned}\hat{x}_f(k) &= \hat{A}_f(h) \hat{x}_f(k-1) + B u(k-1) \\ \hat{y}_f(k) &= C \hat{x}_f(k)\end{aligned}\tag{6.45}$$

where the matrix $\hat{A}_f(h)$ has the same structure as A_f in EQ (6.40), but different parameters, $\hat{a}_{fi}(h)$, $i = 1, 2, \dots, n$, where h is defined in EQ (5.80). It represents the time step at which the estimates are updated.

Because $\hat{a}_{fi}(h) = \hat{\theta}^i(h)$, $\bar{a}_{fi}(h) = \hat{\theta}_{max}^i(h)$ and $\underline{a}_{fi}(h) = \hat{\theta}_{min}^i(h)$, from EQ (5.75) and EQ (5.76), one can write

$$\begin{aligned}\underline{a}_{fi}(h) &< a_{fi} < \bar{a}_{fi}(h) \\ \underline{a}_{fi}(h) &< \hat{a}_{fi} < \bar{a}_{fi}(h) \\ i &= 1, 2, \dots, n\end{aligned}\tag{6.46}$$

and

$$\hat{a}_{fi}(h) = \frac{\bar{a}_{fi}(h) + \underline{a}_{fi}(h)}{2}\tag{6.47}$$

Based on the above equations, by defining:

$$\bar{A}_f(h) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -\bar{a}_{fn}(h) & -\bar{a}_{f(n-1)}(h) & \dots & \dots & -\bar{a}_{f1}(h) \end{bmatrix} \quad (6.48)$$

and

$$A_f(h) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -a_{fn}(h) & -a_{f(n-1)}(h) & \dots & \dots & -a_{f1}(h) \end{bmatrix} \quad (6.49)$$

one can obtain the following relationships:

$$\begin{aligned} \|A_f(h)\|_F &< \|A_f\|_F < \|\bar{A}_f(h)\|_F \\ \|A_f(h)\|_F &< \|\hat{A}_f(h)\|_F < \|\bar{A}_f(h)\|_F \end{aligned} \quad (6.50)$$

Defining the estimation error matrix as $E(h)$, and the estimation error matrix bound as $E_b(h)$, where

$$E(h) = A_f - \hat{A}_f(h) = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \\ e_n(h) & e_{n-1}(h) & \dots & \dots & e_1(h) \end{bmatrix} \quad (6.51)$$

and

$$E_b(h) = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \\ e_n^b(h) & e_{n-1}^b(h) & \dots & \dots & e_1^b(h) \end{bmatrix} \quad (6.52)$$

where $e_i(h) = \hat{a}_{fi}(h) - a_{fi}(h)$. From EQ (5.77), one can denote that

$$e_i^b(h) = \left| \sigma(h-1) [P_{(i,i)}(h)]^{1/2} \right|, i = 1, 2, \dots, n \quad (6.53)$$

It is clear that $|e_i(h)| < e_i^b(h)$, therefore,

$$\|E(h)\|_F < \|E_b(h)\|_F \quad (6.54)$$

Finally, a bounded estimated post-fault system model is obtained, and the parameter estimation error is also bounded. Based on this model, the state-feedback control becomes:

$$u(k-1) = -K_f(h) x_f(k-1) + v(k-1) \quad (6.55)$$

where $v(k-1)$ is the reference input, and $K_f(h)$ is the reconfigurable control gain. It should be pointed out that the state feedback gain $K_f(h)$ is calculated only at every step in h . In this sense, h can be referred to as the reconfiguration step.

For every h , $K_f(h)$ can be designed so that the closed-loop system eigenvalues based on the estimated model, $\lambda_i[\hat{A}_f(h) + BK_f(h)]$, $i = 1, 2, \dots, n$ are placed at the prescribed locations (closed-loop system eigenvalues under normal operations), i.e.

$$\lambda_i^f = \lambda_i[\hat{A}_f(h) + BK_f(h)] = \lambda_i[A + BK_o] = \lambda_i^o \quad (6.56)$$

where K_o is the state-feedback gain for the original nominal system.

There exist many design techniques for assigning the closed-loop system eigenvalues using a state feedback. In fact, one can use the famous Ackermann's formula for solving this problem, [10]:

$$K_f(h)^T = W_f^T(h) \cdot [\hat{A}_f(h) - \lambda_1^o I] \cdot [\hat{A}_f(h) - \lambda_2^o I] \dots [\hat{A}_f(h) - \lambda_n^o I] \quad (6.57)$$

where $W_f^T(h) = [0 \ 0 \ \dots \ 1] [B \ \hat{A}_f(h)^2 B \ \dots \ \hat{A}_f(h)^{n-1} B]^{-1}$.

With such $K_f(h)$, the eigenvalues of the closed-loop system become:

$$\lambda_i [A_f + BK_f(h)] = \lambda_i [\hat{A}_f(h) + BK(h) + E(h)] \quad (6.58)$$

From the Bauer-Fike theorem, [11], by denoting $\hat{A}_{fc}(h) = \hat{A}_f(h) + BK_f(h)$, and $A_{fc}(h) = A_f + BK_f(h)$, it can be shown that:

$$|\lambda_i [A_{fc}(h)] - \lambda_i [\hat{A}_{fc}(h)]| \leq \kappa(\hat{A}_{fc}(h)) \|E(h)\|_p \quad (6.59)$$

where $\kappa(\cdot)$ is the condition number which is related to the matrix $\hat{A}_{fc}(h)$. $\|\cdot\|_p$ is the Hölder matrix norm, which is defined as follows:

$$\text{for } A = [a_{i,j}] \in \mathbb{R}^{n \times n}, \|A\|_p = \left(\sum_{i,j=1}^n |a_{i,j}|^p \right)^{\frac{1}{p}} \quad \forall p \in [1, \infty) \quad (6.60)$$

It should be mentioned that when $p = 2$, the above norm becomes the Frobenius norm, which is often used in robust control design techniques. Therefore, in this case, EQ (6.59) can also be written as:

$$\left| \lambda_i [A_{fc}(h)] - \lambda_i [\hat{A}_{fc}(h)] \right| \leq \kappa(\hat{A}_{fc}(h)) \|E(h)\|_F \quad (6.61)$$

Lemma 6.1 *The stability of the closed-loop post-fault system is guaranteed if the estimation error bound satisfies the following condition:*

$$\|E_b(h)\|_F \leq \frac{1}{\kappa(\hat{A}_{fc})} \left(1 - \max_i \left| \lambda_i [\hat{A}_{fc}(h)] \right| \right) \quad (6.62)$$

Proof:

From EQ (6.59), it can be obtained that:

$$\left| \lambda_i [A_{fc}(h)] \right| - \left| \lambda_i [\hat{A}_{fc}(h)] \right| \leq \left| \lambda_i [A_{fc}(h)] - \lambda_i [\hat{A}_{fc}(h)] \right| \leq \kappa(\hat{A}_{fc}(h)) \|E(h)\|_F \quad (6.63)$$

Therefore,

$$\left| \lambda_i [A_{fc}(h)] \right| \leq \left| \lambda_i [\hat{A}_{fc}(h)] \right| + \kappa(\hat{A}_{fc}(h)) \|E(h)\|_F \leq \left| \lambda_i [\hat{A}_{fc}(h)] \right| + \kappa(\hat{A}_{fc}(h)) \|E_b(h)\|_F \quad (6.64)$$

By substituting $\|E_b(h)\|_F$ from EQ (6.62) into the right term of EQ (6.64), it can be seen clearly that the following inequality is true:

$$\left| \lambda_i [\hat{A}_{fc}(h)] \right| + \kappa(\hat{A}_{fc}) \|E_b(h)\|_F \leq 1 - \left(\max_i \left| \lambda_i [\hat{A}_{fc}(h)] \right| - \lambda_i [\hat{A}_{fc}(h)] \right) \leq 1 \quad (6.65)$$

Therefore, from EQ (6.64), the eigenvalues of the true post-fault system will satisfy:

$$\left| \lambda_i [A_{fc}(h)] \right| \leq 1 \quad (6.66)$$

Hence, the reconfigured closed-loop system is stable.

□

2. Parametric space method based on the robust pole placement technique:

A reconfigurable state feedback controller can also be synthesized using a parametric space based pole placement technique in a straightforward way.

In this case, the closed-loop representation of the estimated post-fault system model with the state feedback controller $K_f(h) = [k_n(h) k_{n-1}(h) \dots k_1(h)]$ can be written as:

$$\hat{x}_f(k) = [\hat{A}_f(h) - BK_f(h)] \hat{x}_f(k-1) + Bv(k-1) \quad (6.67)$$

where

$$\begin{aligned} & \hat{A}_f(h) - BK_f(h) \\ &= \begin{bmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ -(\hat{a}_{fn}(h) + k_n(h)) & -(\hat{a}_{f(n-1)}(h) + k_{n-1}(h)) & \dots & -(\hat{a}_{f1}(h) + k_1(h)) \end{bmatrix} \end{aligned} \quad (6.68)$$

The characteristic polynomial of the above system can then be readily calculated as follows:

$$\begin{aligned} \hat{\phi}(q, h) &= \det \{ qI - [\hat{A}_f(h) - BK_f(h)] \} \\ &= q^n + (\hat{a}_{f1}(h) + k_1(h)) q^{n-1} + \dots \\ &\quad + (\hat{a}_{f(n-1)}(h) + k_{n-1}(h)) q + (\hat{a}_{fn}(h) + k_n(h)) \end{aligned} \quad (6.69)$$

where q is a factor that $y(k-1) = q \cdot y(k)$. Similarly, the closed-loop characteristic polynomial of the true system can also be obtained:

$$\begin{aligned} \phi(q, h) &= q^n + (a_{f1}(h) + k_1(h)) q^{n-1} + \dots \\ &\quad + (a_{f(n-1)}(h) + k_{n-1}(h)) q + (a_{fn}(h) + k_n(h)) \end{aligned} \quad (6.70)$$

By defining:

$$\begin{aligned} \Phi_I(q, h) = & q^n + [a_{f1}(h) + k_1(h), \bar{a}_{f1}(h) + k_1(h)] q^{n-1} + \dots \\ & + [a_{fn}(h) + k_n(h), \bar{a}_{fn}(h) + k_n(h)] \end{aligned} \quad (6.71)$$

where Φ_I is an interval polynomial. It can be seen that:

$$\begin{aligned} \hat{\phi}(q, h) &\in \Phi_I(q, h) \\ \phi(q, h) &\in \Phi_I(q, h) \end{aligned} \quad (6.72)$$

Clearly, the problem of designing a fault tolerant control system becomes the synthesis of feedback gains to stabilize the above interval characteristic polynomial.

There exist many robust control schemes which can deal with systems with parametric uncertainties in terms of parameter bounds [12][13]. First of all, a Schur stable monic polynomial $\phi(q)$ with the desired eigenvalues is introduced as follows, and such a polynomial is called the nominal reference polynomial:

$$\phi(q) = q^n + g_1 q^{n-1} + g_2 q^{n-2} + \dots + g_n \quad (6.73)$$

For this polynomial, the maximal upper and lower bounds of the coefficients can be calculated so that the consequent interval polynomial is also Schur stable [12]. This stable interval polynomial is written as follows:

$$\Psi_I(q) = q^n + [\underline{g}_1, \bar{g}_1] q^{n-1} + [\underline{g}_2, \bar{g}_2] q^{n-2} + \dots + [\underline{g}_n, \bar{g}_n] \quad (6.74)$$

From EQ (6.69) and EQ (6.74), the elements of the feedback gain $k_i(h)$ can be chosen such that:

$$k_i(h) + \hat{a}_{fi}(h) = \frac{\underline{g}_i + \bar{g}_i}{2} \quad i = 1, 2, \dots, n \quad (6.75)$$

i.e.

$$k_i(h) = \frac{\underline{g}_i + \bar{g}_i}{2} - \hat{a}_{fi}(h) \quad (6.76)$$

By using such feedback gains, the stability of the above polynomial can be guaranteed in the following lemma.

Lemma 6.2: Let $e_i^b(h) = \left| \sigma_{h-1}(P_h(i, i))^{1/2} \right|$, the closed-loop system characteristic polynomial, i.e. EQ (6.70) is guaranteed to be Schur stable if

$$e_i^b(h) \leq \frac{\bar{g}_i - \underline{g}_i}{2} \quad (6.77)$$

Proof:

From EQ (6.76), the coefficients of EQ (6.70) can be written as:

$$a_{fi}(h) + k_i(h) = a_{fi}(h) + \frac{\underline{g}_i + \bar{g}_i}{2} - \hat{a}_{fi}(h) = \left(a_{fi}(h) - \hat{a}_{fi}(h) \right) + \frac{\underline{g}_i + \bar{g}_i}{2} \quad (6.78)$$

Since,

$$\left| a_{fi}(h) - \hat{a}_{fi}(h) \right| \leq e_i^b(h) \quad (6.79)$$

Therefore, from EQ (6.78), it can be obtained that,

$$\frac{\underline{g}_i + \bar{g}_i}{2} - e_i^b(h) \leq a_{fi}(h) + k_i(h) \leq \frac{\underline{g}_i + \bar{g}_i}{2} + e_i^b(h) \quad (6.80)$$

It is clear that, if EQ (6.77) is satisfied, it can be obtained that,

$$\underline{g}_i = \frac{\underline{g}_i + \bar{g}_i}{2} - \frac{\bar{g}_i - \underline{g}_i}{2} \leq a_{fi}(h) + k_i(h) \leq \frac{\underline{g}_i + \bar{g}_i}{2} + \frac{\bar{g}_i - \underline{g}_i}{2} = \bar{g}_i \quad (6.81)$$

It implies EQ (6.70) is stable.

□

Now the reconfigurable control system has been effectively synthesized based on the information about the post-fault system provided by the FDI scheme. The proposed reconfigurable control is robust to the imprecise post-fault system model at early stages of fault identification, so that the control reconfiguration can be switched into action promptly. As more data becomes available, tighter bounds will be obtained, consequently, better control can be achieved. Such an approach to fault tolerant control is consistent with the design objectives of active FTCS illustrated in Chapter 2, and the philosophy of the graceful degradation, i.e. maintain the most critical system properties (high priority design objectives) first, and recover the secondary system performance as much as possible gradually.

From the condition posed in Lemma 6.1 and Lemma 6.2, it can be observed that the stability of the resulting closed-loop system depends on the size of estimated uncertainty bounds from the FDI scheme. If the bounds are too large, the stability of the closed-loop system may not be guaranteed. Therefore, a certain amount of time should be allocated to the bounding parameter estimation scheme so that a suitable bound is obtained for the calculation of the stabilizing feedback gains.

6.4 Design Example: Active Fault Tolerant Control of a Lab-Scale Three-Tank System

6.4.1 System description

A picture of a lab-scale three-tank system is shown in Figure 6.3.

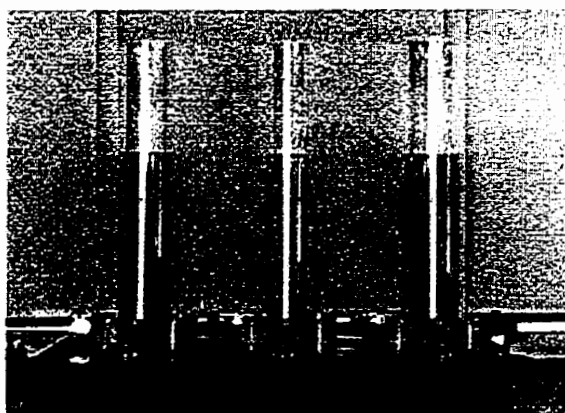


Figure 6.1 A lab-scale three-tank system

An illustrative diagram of this tank system is depicted in Figure 6.4. The system consists of three tanks connected in serial, labelled as tank 1, tank 2, and tank 3. There are two pumps in the system which can fill tank 1 and tank 3 independently. Therefore the level of tank 2 can only be regulated indirectly through the adjacent tanks. In other words, the system has two independent inputs. There is a pressure sensor located at the bottom of each tank for level measurement.

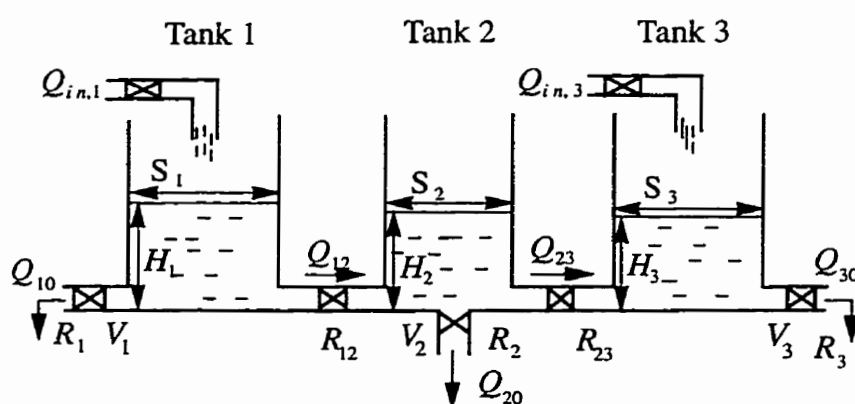


Figure 6.2 An illustrative diagram of the three-tank system

For this system, the design objective is to maintain the liquid level of the tank 2 at a desired height and to keep the changes of the liquid level within a certain limit in the presence of large disturbances or process faults. Thus, the system has one output, i.e. the liquid level in tank 2. Clearly, the system has one degree of actuator redundancy.

The three-tank system has several unique characteristics that one should bear in mind during the controller design:

- (1) Under no circumstances is the spill-over allowed to occur in any tank. Therefore, one should particularly be careful about the transients in the system;
- (2) The drainage rates of the tanks are uncontrollable in our setup;
- (3) As far as tank 2 is concerned, tanks 1 and 3 (with their respective pumps) can be viewed as actuators. However, since the dynamics of these two tanks are very comparable to that of tank 2, we should model them as a part of the system;
- (4) Tanks 1 and 3 have identical diameters, and their locations in the system are symmetric with respect to tank 2. Thus, the actuator redundancy is in the form of *uniform* redundancy.

In this example, we will specifically demonstrate how to design an active FTCS against process faults. The fault considered is the leakage of tank 2 occurring in the draining valve, V_2 , which can be modelled by an abrupt change in the flow resistance R_2 .

The parameters and the variables of the system are given as follows:

S_1 : Cross-sectional area of the tank 1 ($8.107 \times 10^{-3} m^2$)

S_2 : Cross-sectional area of the tank 2 ($4.560 \times 10^{-3} m^2$)

S_3 : Cross-sectional area of the tank 3 ($8.107 \times 10^{-3} m^2$)

ρ : Density of the liquid (water, $1.0 kg/m^3$)

H_i : Liquid level of the tank i , $i = 1, 2, 3$ (m)

$Q_{in,i}$: Liquid inlet flow rate from the pump i , $i = 1, 2, 3$ (m^3/s)

Q_{i0} : Liquid drainage rate from the tank i , $i = 1, 2, 3$ (m^3/s)

Q_{ij} : Liquid flow rates between tanks i and j (m^3/s)

R_i : Drainage resistance of the valve i , (kg/m^5)

R_{ij} : Flow resistance between the tanks i and j , $i, j = 1, 2, 3$ (kg/m^5)

From the law of mass conservation, we can write out the dynamic relationships between the height of the liquid levels and the inlet and outlet flow rates as follows:

$$\begin{aligned} S_1 \frac{dH_1(t)}{dt} &= Q_{in,1}(t) - Q_{10}(t) - Q_{12}(t) \\ S_2 \frac{dH_2(t)}{dt} &= Q_{12}(t) - Q_{23}(t) - Q_{20}(t) \\ S_3 \frac{dH_3(t)}{dt} &= Q_{in,3}(t) + Q_{23}(t) - Q_{30}(t) \end{aligned} \quad (6.82)$$

where

$$\begin{aligned} Q_{10}(t) &= \kappa_1 \sqrt{g \cdot H_1(t)} \\ Q_{20}(t) &= \kappa_2 \sqrt{g \cdot H_2(t)} \\ Q_{30}(t) &= \kappa_3 \sqrt{g \cdot H_3(t)} \\ Q_{12}(t) &= \kappa_{12} \operatorname{sgn}(H_1(t) - H_2(t)) \sqrt{g \cdot |H_1(t) - H_2(t)|} \\ Q_{23}(t) &= \kappa_{23} \operatorname{sgn}(H_2(t) - H_3(t)) \sqrt{g \cdot |H_2(t) - H_3(t)|} \end{aligned} \quad (6.83)$$

and the parameters are defined as:

$$\kappa_1 = \frac{\rho}{R_1} \quad \kappa_2 = \frac{\rho}{R_2} \quad \kappa_3 = \frac{\rho}{R_3} \quad \kappa_{12} = \frac{\rho}{R_{12}} \quad \kappa_{23} = \frac{\rho}{R_{23}} \quad (6.84)$$

where g is the acceleration of gravity. Substituting EQ (6.83) into EQ (6.82), one can obtain the following equation to describe the coupled tank system:

$$\begin{aligned} \frac{dH_1(t)}{dt} &= -\frac{\kappa_1}{S_1} \sqrt{g \cdot H_1(t)} - \frac{\kappa_{12}}{S_1} \operatorname{sgn}(H_1(t) - H_2(t)) \sqrt{g \cdot |H_1(t) - H_2(t)|} + \frac{Q_{in,1}}{S_1} \\ \frac{dH_2(t)}{dt} &= \frac{\kappa_{12}}{S_2} \operatorname{sgn}(H_1(t) - H_2(t)) \sqrt{g \cdot |H_1(t) - H_2(t)|} \\ &\quad - \frac{\kappa_{23}}{S_2} \operatorname{sgn}(H_2(t) - H_3(t)) \sqrt{g \cdot |H_2(t) - H_3(t)|} - \frac{\kappa_2}{S_2} \sqrt{g \cdot H_2(t)} \\ \frac{dH_3(t)}{dt} &= \frac{\kappa_{23}}{S_3} \operatorname{sgn}(H_2(t) - H_3(t)) \sqrt{g \cdot |H_2(t) - H_3(t)|} - \frac{\kappa_3}{S_3} \sqrt{g \cdot H_3(t)} + \frac{Q_{in,3}}{S_3} \end{aligned} \quad (6.85)$$

Clearly, the system is non-linear. When linearized around an operating point (h_{10}, h_{20}, h_{30}) (it is assumed that $h_{10} > h_{20} > h_{30}$), the following linear model can be obtained:

$$\begin{aligned} \begin{bmatrix} \Delta \dot{H}_1(t) \\ \Delta \dot{H}_2(t) \\ \Delta \dot{H}_3(t) \end{bmatrix} &= \begin{bmatrix} -\alpha_1 \kappa_1 - \alpha_{12} \kappa_{12} & \alpha_{12} \kappa_{12} & 0 \\ \alpha_{21} \kappa_{12} & -\alpha_2 \kappa_2 - \alpha_{21} \kappa_{12} - \alpha_{23} \kappa_{23} & \alpha_{23} \kappa_{23} \\ 0 & \alpha_{32} \kappa_{23} & -\alpha_3 \kappa_3 - \alpha_{32} \kappa_{23} \end{bmatrix} \begin{bmatrix} \Delta H_1(t) \\ \Delta H_2(t) \\ \Delta H_3(t) \end{bmatrix} \\ &\quad + \begin{bmatrix} \frac{1}{S_1} & 0 \\ 0 & 0 \\ 0 & \frac{1}{S_3} \end{bmatrix} \begin{bmatrix} Q_{in1} \\ Q_{in3} \end{bmatrix} \end{aligned} \quad (6.86)$$

where

$$\begin{aligned}
\alpha_1 &= \frac{1}{2S_1\sqrt{h_{10}/g}} & \alpha_2 &= \frac{1}{2S_2\sqrt{h_{20}/g}} & \alpha_3 &= \frac{1}{2S_3\sqrt{h_{30}/g}} \\
\alpha_{12} &= \frac{1}{2S_1\sqrt{|h_{10}-h_{20}|/g}} & \alpha_{21} &= \frac{1}{2S_2\sqrt{|h_{10}-h_{20}|/g}} & & \\
\alpha_{23} &= \frac{1}{2S_2\sqrt{|h_{20}-h_{30}|/g}} & \alpha_{32} &= \frac{1}{2S_3\sqrt{|h_{20}-h_{30}|/g}} & &
\end{aligned} \tag{6.87}$$

So far we have obtained the mathematical model of the whole tank system depicted in Figure 6.4. In fact, in this design example, the drainage of tank 1, tank 2 and tank 3 are assumed to be zero under normal operation, i.e. outlet valves V_1 , V_2 and V_3 are closed. In this case, $R_1 = R_2 = R_3 = \infty$, therefore, $Q_{10} = Q_{20} = Q_{30} = 0$ in EQ (6.82). It is assumed that the initial water levels are $h_{10} = h_{30} = 0.25 (m)$, and $h_{20} = 0.2 (m)$. Flow resistances between the adjacent tanks are $R_{12} = 1.96 \times 10^5 (kg/m^5)$ and $R_{23} = 2.00 \times 10^5 (kg/m^5)$. By substituting all the physical parameters in EQ (6.86), one can write the following linearized tank system model under normal operation:

$$\begin{aligned}
\begin{bmatrix} \Delta \dot{H}_1(t) \\ \Delta \dot{H}_2(t) \\ \Delta \dot{H}_3(t) \end{bmatrix} &= \begin{bmatrix} -0.0044 & 0.0044 & 0 \\ 0.0078 & -0.0156 & 0.0078 \\ 0 & 0.0044 & -0.0044 \end{bmatrix} \begin{bmatrix} \Delta H_1(t) \\ \Delta H_2(t) \\ \Delta H_3(t) \end{bmatrix} \\
&+ \begin{bmatrix} 123.3502 & 0 \\ 0 & 0 \\ 0 & 123.3502 \end{bmatrix} \begin{bmatrix} Q_{in1} \\ Q_{in3} \end{bmatrix}
\end{aligned} \tag{6.88}$$

The plant dynamic fault is modelled as leakage in tank 2, i.e.

$R_2 = \infty \rightarrow R_2 = 1.0 \times 10^3 (kg/m^5)$. Therefore, under the system initial operating condition, the system model under such a fault becomes:

$$\begin{bmatrix} \Delta \dot{H}_1(t) \\ \Delta \dot{H}_2(t) \\ \Delta \dot{H}_3(t) \end{bmatrix} = \begin{bmatrix} -0.0044 & 0.0044 & 0 \\ 0.0078 & -0.0967 & 0.0078 \\ 0 & 0.0044 & -0.0044 \end{bmatrix} \begin{bmatrix} \Delta H_1(t) \\ \Delta H_2(t) \\ \Delta H_3(t) \end{bmatrix} + \begin{bmatrix} 123.3502 & 0 \\ 0 & 0 \\ 0 & 123.3502 \end{bmatrix} \begin{bmatrix} Q_{in1} \\ Q_{in3} \end{bmatrix} \quad (6.89)$$

From the above system model, it is clear that the leakage of the tank 2 has caused the changes in the system matrix, A , by noticing the value of the second element on the diagonal changes from -0.0156 to -0.0967 . Such a fault belongs to the class of system dynamic faults. For this system, an active fault tolerant controller is implemented. The control system diagram is depicted in Figure 6.5. It includes an on-line fault detection and identification module and a reconfigurable control module.

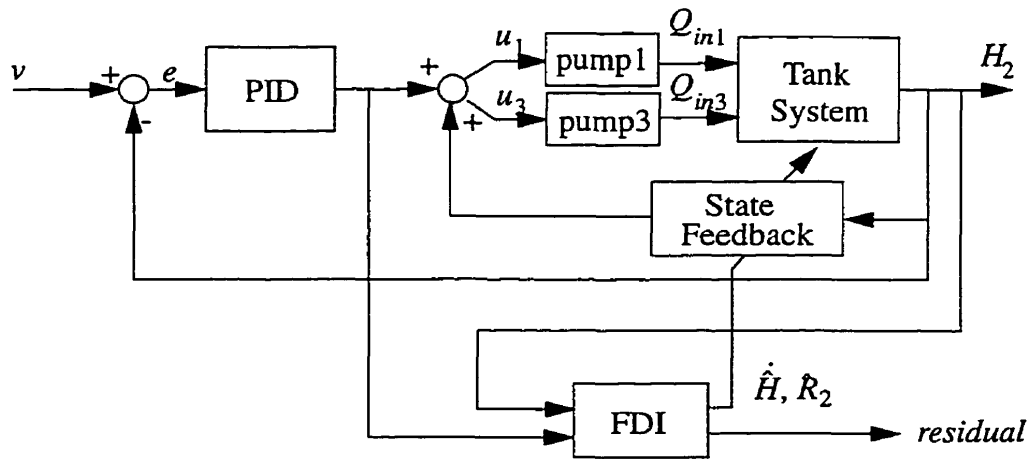


Figure 6.5 The system diagram of fault tolerant three-tank control system

The on-line fault detection and identification scheme is used to detect the occurrence of the leakage, and identify its location and size. The variation rate of the tank 2 liq-

liquid level is estimated on-line, and can be used to estimate the outlet flow resistance ratio of the failed valve. A reconfigurable state-feedback control in the inner loop is used to compensate for the fault-induced system dynamic change, the feedback gain is updated based on the identified fault information, $\hat{R}_2$. To maintain the liquid level after the fault is compensated, a *PID* controller is implemented in the outer-loop.

6.4.2 Experimental results

In order to demonstrate the effectiveness of the proposed active fault tolerant control system, several experiments have been conducted. First of all, the system step response using a conventional control (without FDI and reconfigurable control) is examined, then the system response using the fault tolerant control is examined and compared with the response using conventional control. The results are shown in Figure 6.6.

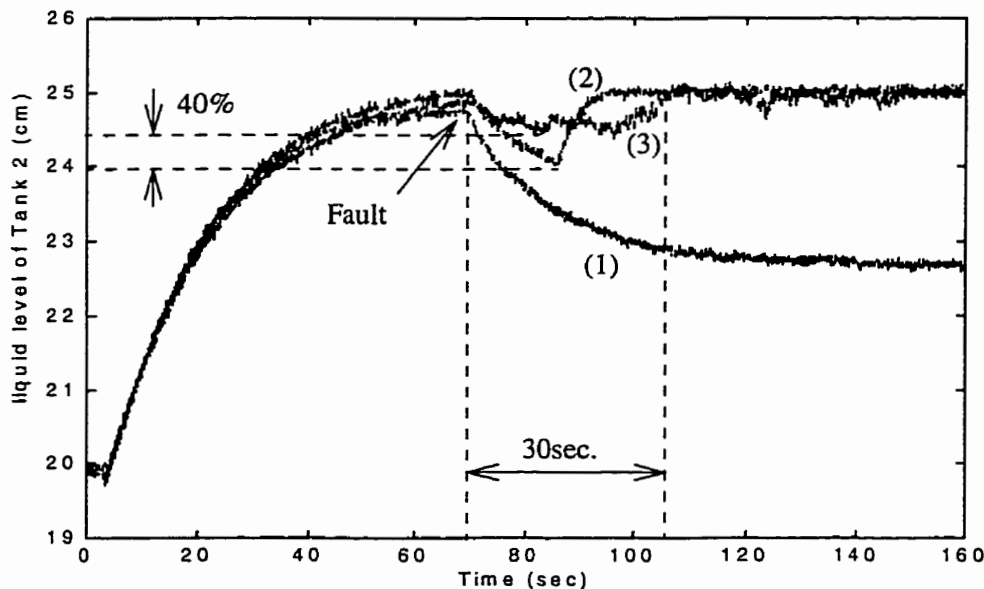


Figure 6.6 System responses under the leakage fault: (1) conventional control; (2) one-step reconfigurable control; (3) multi-step reconfigurable control

The input command of system is to add water so that the liquid level changes from 20 cm to 25 cm. The leakage fault is introduced at $t=70$ sec. From the response labelled (1), it is clear that by using a conventional control, the water level keeps decreasing once the leakage occurs and can never get back to the desired level. However, by using an active fault tolerant control, the occurrence of the fault is detected by an on-line fault detection module, and the size of the fault (value of R_2) is estimated, based on such information, the state-feedback gain is reconfigured to compensate for the fault-induced dynamic changes, finally, water level is brought back to the desired level after about 20 - 30 sec's transients. (see response labelled (2) and (3)).

It should be mentioned that there are some differences between response (2) and response (3), especially, during the transients right after the fault occurrence. For response labelled (2), an one-step reconfigurable control is used, meaning that the controller is only reconfigured once based on the final FDI result. The FDI module, in this case, only provides the reconfigurable control with the fault information after the estimate has converged. Response (3) is obtained by using a multi-step reconfigurable control. In this case, the on-line fault identification module calculates the post-fault value of R_2 in real-time and provides the reconfigurable control module with updated fault information data, and the controller is updated correspondingly based on this data. The FDI and reconfigurable control work in a piecewise continuous fashion, until the liquid level is completely recovered.

By comparing the multi-step reconfigurable control with the one-step reconfigurable control, it is clear that the former responds to the fault much faster, and therefore, the decaying rate is more sluggish than that using a one-step reconfigurable control. In other words, the system performance degrades less drastically. Effectively, the hard deadline is extended further. By observing response (3), although the transients last longer (about 30 sec.), the peak amplitude of the transients is much less than that from response (2) (about 40% less). However, it needs to be pointed out that there are more transients

caused by the control reconfiguration process in the case of multi-step reconfigurable control.

6.5 Conclusion

In this chapter, design aspects of active FTCS are examined. A new design scheme for a reconfigurable control system is proposed. Together with a new bounding parameter estimation based fault identification scheme proposed in Chapter 5, an integrated design for active FTCS is accomplished. The proposed method has been applied to the design of a lab-scale fault tolerant three-tank system. The experimental results are presented to demonstrate the effectiveness of this new active fault tolerant control strategy.

6.6 Bibliography

- [1] Z. Gao and P. J. Antsaklis, "Stability of the pseudo-inverse method for reconfigurable control systems," *International Journal of Control*, vol. 53, pp. 717-729, 1991.
- [2] Z. Gao and P. J. Antsaklis, "On stable solutions of the one- and two-sided model following problems", *IEEE Trans. on Automatic Control*, Vol. 34, No. 9, 1989.
- [3] J. Jiang, "Reconfigurable control systems based on eigenstructure assignments," *International Journal of Control*, vol. 59, pp. 395-410, 1994.
- [4] A. J. Ostroff, "Techniques for accommodating control effector failures on a mildly statically unstable airplane," *Proc. of American Control Conference*, pp. 906 - 903, 1985.
- [5] G. W. Stewart, *Introduction to Matrix Computations*, Academic Press, 1973.
- [6] Z. Gao, *Reconfigurable Control Systems: Analysis and Design*, Ph.D dissertation, pp.14 - 29, 1991.

- [7] H. Erzberger, "Analysis and design of model following control systems by state space techniques," *Proc. of JACC*, pp.572-581, 1968.
- [8] A. N. Andry, E. Y. Shapiro and J. C. Chung, "Eigenstructure assignment for linear systems," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 19, 1983, pp. 711-729.
- [9] L. Ljung, *System Identification: Theory for the User*, Prentice Hall, Englewood Cliffs. NJ, 1987.
- [10] J. E. Ackermann, *Robust Control: Systems with Uncertain Physical Parameters*, Springer-Verlag, New York, 1993.
- [11] A. Weinmann, *Uncertain Models and Robust Control*, Springer-Verlag, New York, 1991.
- [12] S. P. Bhattacharyya, H. Chapellat and L. H. Keel, *Robust Control - The Parametric Approach*, Prentice Hall, NJ. 1995.
- [13] Q. Zhao and J. Jiang, "Reliable state-feedback control system design against actuator failures," *Automatica*, vol. 34, no. 10, pp. 1267 - 1272, 1998.

Conclusions and Future Work

7.1 Conclusions

A new class of control systems, called Fault Tolerant Control Systems (FTCS), has been studied thoroughly in this thesis. Different from conventional control systems, the ultimate goal of Fault Tolerant Control Systems is to maintain the system stability and acceptable performance not only during normal system operation, but also in the presence of system component faults or failures. There are some special considerations in these systems, such as modelling of faults/failures, design objectives in different system operation periods, time constraints, and performance degradation. Most importantly, a necessary condition for FTCS is the existence of hardware and/or analytical redundancy in the system. In fact, the design of Fault Tolerant Control Systems can be viewed as the management of the system redundancy. From this point of view, FTCS can be classified into passive FTCS and active FTCS. In this thesis, special considerations in FTCS were first examined, and some fundamental characteristics of such systems were explored, so that a better and deeper understanding of FTCS was obtained. Based on this understanding, design issues of passive and active FTCS were investigated. New design methodologies were proposed. In the proposed methods, system redundancy has been utilized to achieve fault tolerance, and its important role was emphasized through the entire design process.

In Chapter 1, the basic concepts of Fault Tolerant Control Systems were introduced along with a thorough review of the development of FTCS and the existing literature.

In Chapter 2, different types of system faults were modelled. Then the design objective of FTCS was examined in depth, along with a discussion of performance degradation in FTCS. Finally, the performance specifications for passive and active FTCS were described.

In Chapter 3, the important concept of system redundancy was fully illustrated. Definitions of actuator and sensor redundancies were provided with emphasis on their physical meanings. Chapters 2 and 3 lay the foundation for the entire thesis. The design of FTCS was then carried out using the framework built in these two chapters.

Design problems of Passive FTCS were discussed in Chapter 4. In this chapter, existing design methods for passive FTCS were reviewed first. A new design method for passive FTCS against actuator and sensor failures was then proposed, where the actuator and sensor redundancies were utilized respectively to achieve fault tolerance. It needs to be pointed out that a unique type of sensor redundancy, namely hybrid sensor redundancy (see Chapters 3 and 4) has been used instead of the dissimilar triple sensor redundancy technique [1] for fault tolerance against sensor failures. The proposed designs were successfully applied to a ball-beam balance system and a lab-scale DC drive system.

In Chapter 5, design issues related to the Fault Detection and Identification (FDI) were discussed. First, two common design techniques based on state estimation and parameter estimation were introduced and compared. Then the important issue of the integration of FDI with reconfigurable control was addressed. Finally a new FDI scheme using the fast state estimation based fault detection scheme and a bounding parameter estimation based fault identification scheme was proposed.

Problems in the design of reconfigurable control systems were examined in Chapter 6. A new design scheme for reconfigurable control systems was proposed. The main contribution of the proposed method was the adequate integration of FDI and the reconfigurable control. A design example of the fault tolerant control of a lab-scale three-tank system was then presented. An active fault tolerant control strategy has been utilized

in the design. Experimental results have demonstrated the effectiveness of the proposed design strategy, the integrated design of FDI and reconfigurable control.

In conclusion, the research work presented in this thesis has covered many important issues in Fault Tolerant Control Systems, from the system modelling and performance specifications to the formulation of system redundancy and control system design. These important issues were thoroughly and deeply examined through numerous theoretical studies and experimental tests. Most importantly, new design methodologies for both passive and active FTCS were developed, the important concept of system redundancy were adequately incorporated in the proposed design.

7.2 Future Works

Since control problems of fault tolerant systems are relatively new, there are many challenging problems remaining in this area. Although some of them have been investigated in this thesis, there still exist many open problems that are worth further examination in the future. Some of these problems are:

1. The performance specification of FTCS and the evaluation of the system allowable space and hard deadline in active FTCS.
2. The stability problem of active FTCS when integrating the FDI scheme and the reconfigurable control system, especially during the short period right after the fault occurrence.
3. The design and analysis of FTCS in the stochastic domain.
4. Reliability analysis of FTCS.

These future works are of extreme importance for the development of FTCS. Many subjects are involved, such as real-time computer control [2], stochastic process modelling [2], stochastic stability analysis [3][4], probability and statistics analysis [5].

Some of the research areas are well-developed and some of them are emerging new technologies. They all have found extensive applications to Fault Tolerant Control Systems. Together with these research areas, Fault Tolerant Control Systems have opened up a promising future to the control system science and technology.

7.3 Bibliography

- [1] K. Suyama, "A new type of reliable control system using decision by majority", *Electronics and Communications in Japan*, Part2, vol. 81, no. 2, pp. 46 - 54, 1998.
- [2] F. G. Shin, C. M. Krishna and Y.-H. Lee, "A unified method for evaluating real-time computer controllers and its applications," *IEEE Trans. on Automatic Control*, vol. AC-30, no. 4, pp. 357-366, 1985.
- [3] H. M. Taylor and S. Karlin, *An Introduction to Stochastic Modelling*, Fl: Academic Press, Orlando, 1984.
- [4] M. Mariton, "Detection delays, false alarm rates and the reconfiguration of control systems," *International Journal of Control*, vol. 49, no. 3, pp. 981-992, 1989.
- [5] Srichander, R. and B. K. Walker, "Stochastic stability analysis for continuous time fault-tolerant control systems," *International Journal of Control*, vol. 57, no. 2, pp. 433-452, 1993.
- [6] R. L. Schaeffer and J. T. McClave, *Probability and Statistics for Engineers*, 3rd., MA: PWS-Kent Publishing, Boston, 1990.

An Algorithm to Compute the Nominal Interval Polynomial

In 1991, Soh, *et.al.* presented a procedure to determine the allowable perturbation of the coefficients of a polynomial $P(s)$ about their nominal values, so that the perturbed polynomial still has all its zeros within a desired region in the open left half s -plane.

Assume that an n th order polynomial family has the following form:

$$\begin{aligned} F(s, \varepsilon) &= s^n + f_1 s^{n-1} + \dots + f_n \\ t_i - \tau_i \varepsilon &\leq f_i \leq t_i + \mu_i \varepsilon \quad i = 1, \dots, n \end{aligned} \quad (\text{A. 1})$$

where t_i is the i th coefficient of the nominal polynomial, and $\varepsilon \geq 0$ is the coefficient perturbation. $\mu_i \geq 0, \tau_i \geq 0$ are the two different weights on perturbation.

Now the objective is to find the largest positive value of ε , named ε_M , so that the polynomial family $F(s, \varepsilon_M)$ has all zeros within the desired region.

By defining $F_j(s, \varepsilon), j = 1, \dots, 2^n$, as the vertex polynomial of $F(s, \varepsilon)$, where its coefficients $f_{j,i} = t_i + \mu_i \varepsilon$ or $f_{j,i} = t_i - \tau_i \varepsilon, i = 1, \dots, n$, it can be written as:

$$F_j(s, \varepsilon) = P_0(s) + \varepsilon P_j(s) \quad (\text{A. 2})$$

where

$$P_0(s) = \sum_{i=0}^n t_i s^{n-i}$$

and

$$P_j(s) = \sum_{i=0}^n w_i s^{n-i} \quad w_i \in \{-\tau_i, \mu_i\} \quad (A. 4)$$

$$j = 1, \dots, 2^n$$

Lemma: Assume D is a desired region in the open left half s -plane, $F(s, \varepsilon)$ has all zeros within the region D if and only if all vertex polynomials $F_j(s, \varepsilon)$, $j = 1, \dots, 2^n$, have all zeros within D .

Proof:

see Lemma 3 in [1].

□

Theorem: Suppose $P_0(s)$ has all zeros within the open left-half s -plane, then, the largest positive perturbation value, ε_M , by which the polynomial family $F(s, \varepsilon)$ have all zeros within the open left-half plane is given by

$$\varepsilon_M = \min \{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{2^n}\} \quad (A. 5)$$

where

$$\varepsilon_0 = \begin{cases} \frac{t_0}{\tau_0} & \tau_0 > 0 \\ +\infty & \tau_0 = 0 \end{cases} \quad (A. 6)$$

and

$$\varepsilon_i = \frac{1}{\lambda_{\max}^+(-R_0^{-1}R_i)}, i = 1, 2, \dots, 2^n \quad (4.11)$$

Proof:

See *Theorem 1* in [1].

□

Here $\lambda_{\max}^+(\cdot)$ denotes the maximum positive real eigenvalue of a matrix. R_0 is associated with the nominal polynomial $P_0(s \cdot je^{j\phi})$, where ϕ is shown in Figure 4.10 in Chapter 4. By writing $P_0(s \cdot je^{j\phi})$ as the following form:

$$P_0(s \cdot je^{j\phi}) = \sum_{i=0}^n b_i s^i + j \sum_{i=0}^n a_i s^i$$

The resultant matrix R_0 is defined as:

$$R_0 = \begin{bmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ b_n & b_{n-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & a_n & \dots & \dots & a_1 & a_0 & \dots & 0 \\ 0 & b_n & \dots & \dots & b_1 & b_0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

Similarly, the matrices R_i , $i = 1, 2, \dots, 2^n$ can be obtained from the complex polynomials $P_i(s \cdot je^{j\phi})$, $i = 1, 2, \dots, 2^n$.

Bibliography

- [1] C. B. Soh, H. C. Goh and C. K. Teo, "Invariance of the dynamic properties of a linear continuous time system," *International Journal of Systems Science*, Vol. 22, No.9, pp. 1637-1646, 1991.