Robust Fault Detection and Isolation of Nonlinear Systems with Augmented State Models

Von der Fakultät Konstruktions-, Produktions-, und Fahrzeugtechnik der
Universität Stuttgart
zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte Abhandlung

Vorgelegt von

Jochen Aßfalg
aus Biberach a.d. Riß

Hauptberichter: Prof. Dr.-Ing. Frank Allgöwer
Mitberichter: Prof. Dr.-Ing. Steven X. Ding
Mitberichter: Prof. Dr.-Ing. Thomas Parisini

Tag der mündlichen Prüfung: 26. Mai 2009

Institut für Systemtheorie und Regelungstechnik
der Universität Stuttgart
2009

Die vorliegende Arbeit entstand in den Jahren 2004 bis 2009 während meiner Tätigkeit als externer Industriedoktorand am Institut für Systemtheorie und Regelungstechnik der Universität Stuttgart.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. F. Allgöwer für die ausgezeichnete und engagierte Betreuung dieser Arbeit. Die wertvollen Diskussionen und Anregungen, die eingeräumten fachlichen Freiräume sowie das Fundament seines international renommierten Hochschulinstituts haben wesentlich zum Gelingen dieser Arbeit beigetragen. Herrn Prof. Dr.-Ing. S. X. Ding und Herrn Prof. Dr.-Ing. T. Parisini danke ich vielmals für ihr Interesse an meiner Arbeit und die freundliche Übernahme des Mitberichts.

Besonders danke ich ebenfalls Herrn Dr.-Ing. M. Fritz, der meine Arbeit seitens der Robert Bosch GmbH betreut hat und mir dabei den notwendigen Freiraum für meine Forschungen einräumte. Außerdem bedanke ich mich bei den Herren H. M. Heinkel, Dr. M. Hurich und Dr. W. Lehle für ihr lebhaftes Interesse an meiner Arbeit und die hervorragenden Arbeitsbedingungen in deren Fachabteilungen der Robert Bosch GmbH. Den Kolleginnen und Kollegen bei Bosch und am Institut danke ich für das sehr gute Arbeitsklima und die schöne Zeit während unserer Zusammenarbeit.

Ebenfalls danken möchte ich Simon Görke, Carsten Paulus und Christoph Maier, die im Rahmen ihrer Studien- und Diplomarbeiten einen wertvollen Beitrag geleistet haben. Eine besonders wertvolle Hilfe war dabei die umfangreiche Unterstützung von Christoph Maier bei der Implementierung und Simulation der entwickelten Diagnosealgorithmen.

Vor allem danke ich meiner Frau Kerstin und meinen Eltern Birgit und Josef Aßfalg, ohne deren Unterstützung ich diese Arbeit sicherlich so hätte nicht leisten können.

München, Mai 2009 Jochen Aßfalg

Alles Wissen und alle Vermehrung unseres Wissens endet nicht mit einem Schlusspunkt, sondern mit Fragezeichen. *Hermann Hesse*

Contents

Acronyms **ix**

Abstract **xi**

German Summary / Deutsche Zusammenfassung **xiii**

1 Introduction **1**
1.1 Fault Diagnosis, Fault Detection and Isolation 1
1.2 Research Directions of this Thesis 3
1.3 Thesis Outline and Contribution 5

2 Nominal System, Uncertainty, and Fault Representation **7**
2.1 Basic Problem Setup 7
2.2 Fault Term and Captured Fault-Types 9
2.3 Simple Example – DC Actuator System Subject to Faults 13
2.4 Summary 16

3 Augmented State Models for FDI Analysis and Design – Nominal Case **17**
3.1 Nominal Problem Setup 18
3.2 Augmented State Modeling for FDI 19
3.2.1 Fault Modeling by Exosystems 19
3.2.2 Unstructured Augmented State Modeling 21
3.2.3 Structured Augmented-State Modeling 23
3.2.3.1 Switched Fault Representation 23
3.2.3.2 Structured Augmented State Model 23
3.3 Properties of the Structured Augmented System 26
3.4 FDI with Structured Augmented State Models 33
3.5 Example – Sub-Optimal FDI of the DC Actuator System 37
3.5.1 Fault Representation and Fault Scenario 37
3.5.2 Structured Augmented State Model of the DC Actuator System 38

3.5.3 FDI by Using Sub-Optimal IMM-EKF Hybrid Estimation 39
3.5.3.1 Sub-Optimal IMM-EKF Hybrid Augmented State Estimation . . 39
3.5.3.2 Fault Diagnosis by Using the Sub-Optimal IMM-EKF Algorithm 41
3.5.4 Numerical Results 42
3.6 Summary 43

4 Robust FDI with Uncertain Structured Augmented State Models 45
4.1 Uncertain Structured Augmented State Model 46
4.1.1 Uncertainty of the Continuous Part Model 47
4.1.2 Uncertainty of the Discrete Part Model 48
4.1.3 Uncertain Structured Augmented State Model 49
4.2 Nonlinear Set-Valued Augmented State Estimation 50
4.2.1 Notation, Problem Statement, and Exact Solution 50
4.2.2 Extended Set-Valued Estimation 54
4.2.2.1 Notation and Basic Definitions 55
4.2.2.2 Extended Set-Valued Estimator – Algorithm Summary 56
4.2.2.3 Properties of the ESVE 63
4.3 Robust FDI and Nonlinear Set-Valued Augmented State Estimation 64
4.3.1 Basic Setup – Ideal NSVE and Robust FDI 65
4.3.2 Approximate Approach to Robust FDI Using the ESVE Algorithm 67
4.3.2.1 A Simple Robust FDI Scheme (Non-Switching Case) 69
4.3.2.2 Conditions for a Meaningful FDI and Well-Posedness of the Problem 69
4.4 General Robust FDI Scheme (Switching Case) 74
4.5 Example - Robust FDI of the DC Actuator System 78
4.5.1 Fault Representation, Fault Scenario, and Uncertain Structured Augmented State Model 78
4.5.2 Numerical Results 80
4.6 Summary 83

5 Application to the Three-Tank Benchmark 85
5.1 Model of the Three-Tank 86
5.1.1 Fault Representation, Fault Scenario, and Unknown Mode 87
5.1.2 Modeling Uncertainty and Noise Representation 89
5.1.3 Uncertain Structured Augmented State Model of the Three-Tank 89
5.2 Numerical Results 91
5.2.1 Incipient Fault Scenario 92
5.2.2 Abrupt Fault Scenario 93

5.3 Summary 94

6 Conclusions and Outlook **97**

Bibliography **99**

Acronyms

Acronym	Meaning
FDI	fault detection and isolation
rFDI	robust fault detection and isolation
FTC	fault-tolerant control
EKF	extended Kalman filter
UKF	unscented Kalman filter
DD2F	second order divided difference filter
IMM	interacting multiple-model algorithm
NSVE	nonlinear set-valued estimation
ESVE	extended set-valued estimation
MIMO	multi-input multi-output
I/O	input/output
DC	direct current

Abstract

Model-based fault detection and isolation (FDI) is one of the most important fields in system theory and automation. Roughly speaking, FDI aims at finding and backtracking discrepancies between a system's observed behavior (described by its measurements) and its expected behavior (described by its model). Whenever the model used is uncertain, which means that it does not match the real process accurately, the FDI problem becomes particularly challenging. In practical applications, uncertain system representations are not unusual and thus, incorrect fault detection and false diagnosis can only be prevented, if employed FDI algorithms are robust against model uncertainties.

This thesis presents novel modeling, analysis, and synthesis concepts for the robust FDI of nonlinear systems in a discrete-time representation. In the modeling section, a new formalism for the representation of nonlinear systems subject to faults is introduced. The presented model allows the description of a particularly wide class of faulty systems and moves the problems of fault diagnosis and state estimation close together, which would otherwise be different. By exploiting this relationship, novel conditions for linear and nonlinear fault-detectability and -isolability analysis are provided. The proposed conditions are based on well-known observability definitions and can thus be verified by means of established methods from the field of observability analysis. On the basis of the proposed model, the nominal and the Gaussian noisy fault diagnosis problem are expressed as an optimal hybrid state estimation problem. The use of sub-optimal solutions is discussed and illustrated by means of a practical example.

In order to cope with uncertain problem formulations including plant-model-mismatch and unanticipated faults, the suggested modeling formalism is modified. Disturbances, modeling uncertainties, and measurement noise are characterized using unknown-but-bounded exogenous inputs. The unknown-but-bounded uncertainty representation proves to be exceptionally practicable, since no specific and difficult assumptions about the uncertainties have to be met a priori. On the other hand, unforeseen plant operations that are not captured by the model, e.g. unanticipated faults and unexpectedly large disturbances, are lumped in an unknown mode of operation. Based on the resulting uncertain model, a robust FDI algorithm is developed that is capable of diagnosing permanent and intermittent faults and furthermore is able to detect unknown modes of operation.

Robust fault-detection and -isolation conditions are derived, by which the suggested algorithm is guaranteed to determine a meaningful and unique result.

The fault diagnosis methods proposed in this thesis are expressed as algorithms that can be directly implemented and processed in a reasonable time. Several detailed examples, including the three-tank benchmark with unknown-but-bounded modeling uncertainties, demonstrate the properties and the applicability of the proposed methods.

Deutsche Zusammenfassung

Nie zuvor war unsere Gesellschaft in einem derart hohen Maß von der Verfügbarkeit und korrekten Funktion komplexer technischer Systeme abhängig wie heute. International verflochtene Energieversorgungsnetzwerke, Telekommunikationsnetze und Transportsysteme nehmen einen hohen Einfluss auf unsere Wirtschaft und auf unser tägliches Leben. Moderne Fertigungsanlagen, welche sich aus vielen einzelnen, wiederum in sich komplexen Werkzeugmaschinen, Robotern und Transfersystemen zusammensetzen, müssen zur Gewährleistung einer wirtschaftlichen und qualitativ hochwertigen Produktion fehlerfrei funktionieren. Im Automobilbereich stellen immer schärfer werdende Umweltvorschriften wie On-Board Diagnostics II (OBDII) und European On-Board Diagnostics (EOBD) (siehe z.B. (Zimmermann and Schmidgall, 2008)) neue Anforderungen an Steuergerätefunktionalitäten, die eine permanente Betriebsüberwachung von Verbrennungsmotoren und eine zuverlässigen Kontrolle kritischer Abgaswerte gewährleisten müssen. Dies sind nur einige wenige Beispiele, welche den Bedarf neuer Entwicklungen auf dem Gebiet der automatischen Fehlerdiagnose auf beeindruckende Weise demonstrieren.

Automatische Fehlerdiagnosesysteme stellen eine ,,versteckte Technologie" dar, das heißt, wir erfahren nur ihren Nutzen und ihre Auswirkungen, ihre Wirkungsweise bleibt aber meistens unsichtbar. Dennoch begleitet uns diese Technologie in unserem täglichen Leben und die Welt wie wir sie kennen ist ohne Diagnosesysteme nicht mehr vorstellbar. Der Trend zu immer komplexer werdenden technischen Systemen forciert den Einsatz automatischer Diagnosesysteme weiter und rückt deren systematische Entwicklung in den Fokus der modernen systemtheoretischen Forschung.

Fehlerdiagnose, Fehlerdetektion und -isolation

Der Begriff der Fehlerdiagnose bezeichnet im Allgemeinen den *Prozess der Detektion, der Isolation und der Identifikation von möglichen Fehlern* die ein betrachtetes System beeinträchtigen können. Die drei enthaltenen Teilaufgaben werden generell wie folgt beschrieben (Blanke *et al.*, 2003):

- *Fehlerdetektion:* Im Teilschritt der Fehlerdetektion (Fehlererkennung) wird festgestellt ob ein Fehler aufgetreten ist. Welcher Fehler dabei vorgefallen ist, bleibt jedoch unbekannt.

- *Fehlerisolation:* Die Fehlerisolation bestimmt welcher spezielle Fehler vorgefallen ist und erfordert eine genaue Lokalisierung des entstandenen Defekts. Die Amplitude des Fehlers bzw. das Schadensausmaß interessieren hierbei nicht.
- *Fehleridentifikation:* Bei der Fehleridentifikation wird die Amplitude eines vorliegenden Fehlers bestimmt und somit das Ausmaß des resultierenden Schadens abgeschätzt.

Neben dem eigentlichen Diagnoseprozess wird ebenfalls die daraus hervorgehende Erkenntnis als Fehlerdiagnose bezeichnet.

Im Wesentlichen erfolgt eine Fehlerdiagnose indem gemessene Ein- und Ausgangsgrößen eines betrachteten Systems analysiert werden (siehe Abbildung 1). Um eine korrekte und möglichst eindeutige Diagnose zu stellen, wird dabei nach Symptomen gesucht, welche auf die Präsenz bestimmter Fehler hindeuten.

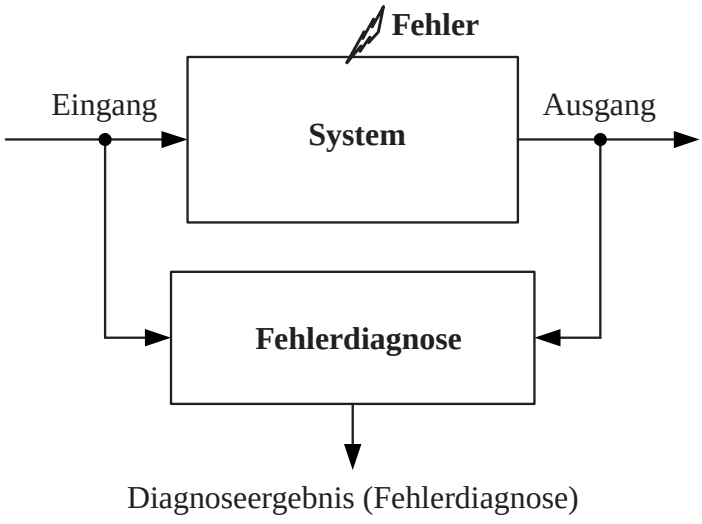


Abbildung 1: Generische Struktur der Fehlerdiagnose.

In der Regel beschränken sich praktische Anwendungen der Fehlerdiagnose auf die Teilaufgaben der *Fehlerdetektion und Fehlerisolation (FDI)*. Die darin gewonnenen Informationen sind allgemein ausreichend, um Maßnahmen wie Systemabschaltungen, Reparaturen oder online ausgeführte Rekonfigurationen des zu diagnostizierenden Systems einzuleiten.

Die Hauptanwendungen der FDI können im Wesentlichen den folgenden drei Aufgabengebieten zugewiesen werden:

- *Systemüberwachung (Monitoring)*. Die automatische Systemüberwachung zielt im Wesentlichen auf sicherheitskritische Systeme wie z.B. Flugzeuge, Kraftwerke und chemische Reaktoren ab. Aber auch in anderen Anwendungen in welchen moderne technische Systeme sicher, umweltverträglich und profitabel betrieben werden müssen, spielt sie eine zentrale Rolle. Um entscheidende Informationen zu einer Einleitung angemessener Fehlerreaktionen,

wie einen Wechsel in den Notlaufbetrieb oder sogar eine Systemabschaltung zu gewinnen, müssen eingetretene Fehler möglichst frühzeitig erkannt werden. Zusätzliche Informationen aus einer Fehlerisolation erlauben weitere Verbesserungen, da mögliche Reaktionen fehlerspezifisch vorgenommen und unnötige Systemausfälle vermieden werden können. Ungeachtet dessen müssen FDI Funktionalitäten die zu einer Systemüberwachung herangezogen werden grundsätzlich online und in Echtzeit ausgeführt werden.

- *Fehlersuche*. In der automatisierten Fehlersuche wird die FDI dazu eingesetzt um die Wartbarkeit zunehmend komplexer und daher auch immer undurchschaubarer werdender Systeme zu verbessern. Automatische Diagnosetester stellen deshalb bereits in vielen Instandhaltungsbereichen, wie beispielsweise im Kfz Servicebereich und der Wartung automatisierungstechnischer Anlagen, einen Standard dar. Selbstverständlich spiegelt sich die an einem realen System wahrgenommene Komplexität stets in dessen modelltechnischer Beschreibung wieder, was wiederum den Entwurf automatischer FDI Funktionen schwierig gestaltet. Da mit steigendem Komplexitätsgrad eines Systems in der Regel auch die Anzahl der potentiellen Fehler zunimmt, stellt bei solchen Systemen insbesondere die Fehlerisolation eine besondere Herausforderung dar. Wohingegen zu einer reinen Systemüberwachung eine online Ausführung zwingend erforderlich ist, kann die FDI zum Zweck der Fehlersuche sowohl online, offline als auch in einem kombinierten on-/offline Ansatz realisiert werden; je nach betrachtetem Problem, dem erzielten Ergebnis und der verfügbaren Rechenleistung.

- *Fehlertolerante Regelung*. Das Hauptaugenmerk der fehlertoleranten Regelung ist die permanente Aufrechterhaltung fundamentaler Systemfunktionen, auch im fehlerhaften Betrieb eines Systems. Die Entwicklung fehlertoleranter Systeme ist ein wichtiger Schritt in die Richtung von autonom funktionierenden Systemen wie sie zum Beispiel in der Robotik, in der unbemannten Luftfahrt und in der Raumfahrt zum Einsatz kommen. Die FDI bildet den Kern einer jeden fehlertoleranten Regelungsfunktion zumal diese im Fehlerfall essentielle Informationen für online (in Echtzeit) ausgeführte Anpassungen des Regelungssystems bereitstellt. Die fehlertolerante Regelung vereint die FDI und die klassische Regelungstechnik und ist eines der vielversprechendsten Gebiete der heutigen systemtheoretischen Forschung.

In all diesen Anwendungsgebieten spielt die automatische FDI eine zentrale Rolle. Systemtheoretische Indikatoren für „Komplexität” wie sie von uns am realen System wahrgenommen wird, sind beispielsweise durch Systemnichtlinearitäten, Mehrgrößenverhalten und durch eine hohe Zustandsdimension gegeben. Die Analyse und der Entwurf von FDI Algorithmen ist für solche Systeme besonders herausfordernd. Dies gilt vor allem dann, wenn ein System in seiner Eigenschaft mehrere dieser Indikatoren vereint. Die Weiterentwicklung bestehender Methoden zu einer diagnosegerichteten Systemanalyse und zum Entwurf automatischer Diagnosefunktionen ist deshalb

unumgänglich, insbesondere angesichts der rapiden Entwicklung zu immer komplexer werdenden technischen Systemen.

Forschungsrichtungen dieser Arbeit

Motiviert durch die vorangehende Diskussion beschäftigt sich diese Arbeit mit der robusten FDI nichtlinearer Systeme auf der Basis zeitdiskreter unsicherer Zustandsmodelle. Die Hauptforschungsrichtung ist die Entwicklung neuer und rechentechnisch realisierbarer Analyse- und Entwurfsmethoden zu einer FDI unsicherer nichtlinearer Systeme. Diese Arbeit beschäftigt sich dabei insbesondere mit Systemen der Form

$$\begin{aligned} x_{k+1} &= f\big(x_k, u_k, \delta_k, w_k\big),\ x_0,\ k \geq 0, \\ y_k &= h\big(x_k, u_k, \delta_k, v_k\big), \end{aligned}$$

beziehungsweise mit entsprechenden zeitkontinuierlichen Formulierungen. Dabei bezeichnet x_k den Zustand, u_k die Eingänge und y_k die Ausgänge des Systems. Die Systemgleichungen sind des Weiteren von den exogenen Eingangsgrößen w_k und v_k abhängig, welche die Einflüsse möglicher Modellunsicherheiten, Störungen und von Messrauschen abbilden. Potentielle Fehler des Systems werden anhand des exogenen Eingangs δ_k dargestellt. Das Signal δ_k kann dabei sowohl in die System- als auch in die Ausgangsgleichung eingehen. Die somit beschriebene Problemklasse ist riesig und umfasst neben einer Vielzahl realer komplexer Systeme (wie nichtlineare Systeme und Mehrgrößensysteme) eine Vielzahl verschiedener Fehler- und Unsicherheitstypen. Verschiedenste Beispiele existieren für die beschriebene Problembklasse in nahezu jedem Anwendungsgebiet, seien es elektrische Maschinen, prozesstechnische Anlagen, Automobile, Flugzeuge und viele mehr.

Das Gebiet der modellbasierten FDI hat in mehreren Jahrzehnten Forschung einen sehr hohen Reifegrad erlangt. Gute Einführungen in diese Thematik und Übersichten zu den aktuellen Methoden sind beispielsweise in (Blanke *et al.*, 2003) und (Ding, 2008) enthalten. Den Großteil der bislang vorhandenen Ergebnisse auf dem Gebiet der FDI stellen lineare Entwurfsmethoden dar, welche im Wesentlichen auf Beobachter-, Paritätsraum- und Parameterschätzverfahren zurückgreifen. Die Anwendung dieser Methoden hat sich bereits vielfach in der Lösung praktischer Diagnoseprobleme bewährt, sowohl an den Hochschulen als auch in der Industrie. Die Systeme, die praktischen FDI Anwendungen zu Grunde liegen, sind jedoch oftmals nichtlinear und erzwingen den Einsatz nichtlinearer Lösungsansätze. Wie es in nachfolgenden Ausführungen der Arbeit noch detaillierter ausgeführt wird, fehlt es aktuell an robusten FDI Ansätzen, welche zu einer Anwendung auf die besonders weitreichende, hier zu Grunde gelegte Klasse nichtlinearer Systeme geeignet sind. Auf der einen Seite existieren nur wenige Ergebnisse und Methoden zu einer Diagnostizierbarkeitsanalyse nichtlinearer Systeme. Jedoch sind praktikable Analysemethoden in der FDI essentiell. Sie ermöglichen, zu bewältigende Diagnoseaufgaben hinsichtlich ihrer Lösbarkeit zu prüfen und

dienen zum Erlangen weiterer grundlegender Informationen, die für eine erfolgreiche FDI dienlich sind. Auf der anderen Seite ist der Entwurf nichtlinearer FDI Algorithmen ein weitreichend offenes Gebiet. Besonders wenige praktisch anwendbare Methoden zur nichtlinearen FDI sind derzeit zu einem robusten Entwurf im Umgang mit meist unvermeidbaren Modellunsicherheiten verfügbar. Ein weiteres, nahezu unbeschrittenes Aufgabengebiet, ist die Behandlung sporadischer und unbekannter Fehler. Diese bewirken zum einen, eine äußerst schwierig handhabbare schaltende Diagnoseumgebung. Zum anderen führen unbekannte Fehler zu unbekannten und daher schwierig bewertbaren Betriebszuständen eines betrachteten Systems.

Diese Arbeit trägt zu der Lösung dieser noch ungelösten Probleme bei. Dabei wird auf dem Lösungsweg in besonderem Maß auf die praktische Anwendbarkeit und die prozessrechentechnische Umsetzbarkeit der vorgeschlagenen Analysemethoden und Algorithmen geachtet. Die Basis des entwickelten FDI-Ansatzes bilden etablierte Ergebnisse aus der Theorie der kontinuierlichen und hybriden Zustandsschätzung, die schrittweise zu einem Baukasten von Analyse- und Entwurfsmethoden zur robusten FDI ausgebaut werden. Die Verbindung dieser sonst so verschiedenen Methodengebiete wird mit Hilfe einer neuen, besonders allgemeingültigen Modellform hergestellt. Weitere theoretische Beiträge dieser Arbeit komplettieren diese Ausgangsbasis zu einem umfassenden und eigenständigen Ansatz zur robusten FDI nichtlinearer Systeme. Aus globaler Sicht stellt diese Arbeit eine vollständige Methodik zur robusten FDI nichtlinearer Systeme bereit, welche am praktischen Nutzer orientiert ist und auf eine weitreichende Klasse praktischer Diagnoseprobleme anwendbar ist.

Gliederung und Forschungsbeiträge der Arbeit

Im Folgenden wird eine Übersicht zu der Gliederung und zu den wesentlichen Forschungsbeiträgen der Arbeit gegeben.

Kapitel 2 – Nominal System, Uncertainty, and Fault Representation (Nominelles System, Modellunsicherheiten und Fehlermodelle) – formuliert die zu Grunde gelegte Problemkonfiguration und führt die bertrachteten Klassen von Systemen, Fehlern und Modellunsicherheiten ein. In diesem Zusammenhang wird eine neue systemtheoretische Definition des Fehlerbegriffs (Definition 2.1) von der DIN Norm 40042 (siehe z.B. (Isermann, 1994)) abgeleitet. Zudem wird ein praktisches Beispiel eines potentiell fehlerhaften Gleichstrommotors eingeführt, welches den Leser in den nachfolgenden Kapiteln als anschauliches Beispiel begleitet (Section 2.3).

Kapitel 3 – Augmented State Models for FDI Analysis and Design - Nominal Case (Erweiterte Zustandsmodelle zur FDI Analyse und Synthese - Nomineller Fall) – stellt einen vollständigen Ansatz zur FDI bereit, welcher die Modellierung, die Analyse und den FDI Entwurf für nominelle

nichtlineare Diagnoseprobleme umfasst. Teile dieses Kapitels basieren auf den Veröffentlichungen (Aßfalg and Allgöwer, 2006*b*) und (Aßfalg and Allgöwer, 2007).

- Strukturiertes erweitertes Zustandsmodell: Ein neuer Ansatz zur Beschreibung potentiell fehlerhafter Systeme wird beschritten. Dieser ist allgemeingültig formuliert und erlaubt die vollständige Darstellung aller, in der Diagnoseliteratur üblich unterschiedenen Fehlertypen (Definition 3.1). Indem das bekannte und praktisch vielfach bewährte Prinzip der Zustandserweiterung zu Grunde gelegt wird, kann das FDI Problem als hybrides (erweitertes) Zustandsschätzproblem formuliert werden (Problem 3.1).

- Bedingungen zur Detektierbarkeit und Isolierbarkeit von Fehlern: Neue Bedingungen zur Detektierbarkeits- und Isolierbarkeitsanalyse von Fehlern werden bereitgestellt (Theorem 3.1 und Theorem 3.2). Dabei basieren beide Bedingungen auf der Beobachtbarkeitseingenschaft in ihrer fundamentalen Definition ununterscheidbarer Zustandspaare. Beide Bedingungen können anhand etablierter Methoden der Beobachtbarkeitsanalyse verifiziert werden. Die hergeleiteten Bedingungen schließen eine konzeptionelle Lücke in der Diagnoseliteratur und stellen praktisch anwendbare Methoden zu einer Diagnostizierbarkeitsanalyse linearer und nichtlinearer Systeme bereit.

- Hybride erweiterte Zustandsschätzung zur FDI: Auf der Basis der hergeleiteten Modellform wird ein Weg aufgezeigt wie eine FDI mit Hilfe bewährter Methoden aus der hybriden Zustandsschätzung berechnet werden kann (Section 3.4).

Kapitel 4 – Robust FDI with Uncertain Structured Augmented State Models (Robuste FDI mit Unsicheren Strukturierten Erweiterten Zustandsmodellen) – behandelt den Entwurf robuster FDI Funktionen. Die Robustheit einer FDI ist genau dann erforderlich, wenn unsichere Modellbeschreibungen des betrachteten Diagnoseproblems die Ausgangsbasis des Entwurfsprozesses bilden.

- Unsicheres Strukturiertes Erweitertes Zustandsmodell: Der nominelle Modellierungsansatz der strukturierten erweiterten Zustandsmodelle wird zu einer Beschreibung unsicherer Probleme ausgeweitet (Definition 3.4). Diese berücksichtigt neben Modellunsicherheiten der System- und Fehlerbeschreibung auch unbekannte und daher unberücksichtigte Fehlerkandidaten. Kontinuierliche Modellunsicherheiten wie sie beispielsweise durch externe Störungen, Modellfehler und Messrauschen verursacht werden, werden anhand von unbekannten aber beschränkten Eingangsgrößen beschrieben. Diese Form der Unsicherheitsbeschreibung ist besonders praktisch und intuitiv anwendbar zumal keine genaue Spezifikation der unbekannten Größen erforderlich ist. Fehler die im Modellierungsprozess unbedacht blieben und deshalb zu diskreten Modellunsicherheiten führen, werden in Form eines zusätzlichen unbekannten Betriebsmodes berücksichtigt.

- Ansatz zur robusten FDI: Zunächst werden einige Hintergrundinformationen und grundlegende Zusammenhänge der nichtlinearen Zustandsmengenschätzung erläutert. Im Anschluss wird ein neuer systemtheoretischer Ansatz entwickelt, der die Verbindung zwischen der Zustandsmengenschätzung und der robusten FDI herstellt. Den Ausgangspunkt hiefür bildet der ideale Lösungsansatz des nichtlinearen Zustandsmengenschätzproblems, auf dessen Basis, der ideale jedoch rechentechnisch nicht umsetzbare Ansatz der robusten FDI hergeleitet wird (Proposition 4.1 und Theorem 4.1). Dieser wird im Anschluss zu einer näherungsweisen, rechentechnisch realisierbaren Lösung weiterentwickelt, welche direkt in einem einfachen Schema zur robusten FDI nicht-schaltender Diagnoseprobleme resultiert (Proposition 4.2 und Theorem 4.2).

- Bedingungen zu einer robusten Fehlerdetektierbarkeit und -isolierbarkeit: Ausgehend von dem näherungsweisen Lösungsansatz werden neue Bedingungen für eine robuste Detektierbarkeit und Isolierbarkeit von Fehlern hergeleitet (Proposition 4.3 und Proposition 4.4, Theorem 4.3 und Theorem 4.4). Eine robuste und nicht-triviale FDI ist genau dann wie vorgeschlagen bestimmbar, wenn diese beiden Bedingungen erfüllt sind.

- Algorithmus zur robusten FDI (schaltender Fall): Intermittierende Fehler, welche während des Diagnoseprozesses (wiederholt) auftreten und verschwinden, sind im Allgemeinen besonders schwierig handhabbar. Dies ist darin begründet, dass solche Fehlertypen eine schaltende Diagnoseumgebung hervorrufen. Als Lösungsansatz dieser schwierigen Problemklasse wird ein neues FDI Verfahren bereitgestellt, welches sowohl in einer schaltenden als auch in einer nicht-schaltenden Diagnoseumgebung angewendet werden kann (Algorithm 4.3). Darüber hinaus ist der vorgeschlagene Algorithmus nachweisbar robust gegenüber Modellunsicherheiten und erlaubt, unter der Voraussetzung bestimmter Systemeigenschaften, eine Detektion und Isolation unbekannter Fehler.

Kapitel 5 – Application to the Three-Tank Benchmark (Anwendung auf das Drei-Tank-Benchmark) – veranschaulicht die entwickelte Entwurfsmethodik anhand eines Anwendungsbeispiels. Hierzu wird das in der Diagnoseliteratur häufig verwendete Beispiel des Drei-Tank Systems herangezogen und zur Veranschaulichung des vorgeschlagenen Modellierungsprinzips, des robusten FDI Entwurfsprozesses sowie zu der Wahl notwendiger Einstellparameter verwendet.

Kapitel 6 – Conclusions and Outlook (Zusammenfassung und Ausblick) – enthält eine Zusammenfassung der Arbeit, diskutiert ihre Ergebnisse und gibt einen Ausblick auf mögliche zukünftige Weiterentwicklungen der behandelten Themen.

Chapter 1

Introduction

As never before, modern society depends on the operational reliability of complex technical systems. Internationally networked power grids, telecommunications networks, and transportation systems exert high influence on our every day life. But also modern production lines consisting of various machine tools, robots, and transfer systems have to be kept in fault-free operation in order to provide for an efficient and high-quality production. In automotive engineering, environmental regulations like On-Board Diagnostics II (OBDII) and European On-Board Diagnostics (EOBD) (see, e.g. (Zimmermann and Schmidgall, 2008)) demand a continuous monitoring of combustion engines and furthermore necessitate a reliable supervision of critical exhaust-gas values. These are just few examples demonstrating the need of new developments in the field of automated diagnostics.

Automatic fault diagnosis constitutes a ”hidden technology”, which means that we experience its benefits and effects, but it remains mostly invisible how it works. Yet these technology accompanies us in our every day life and the world as we know is unimaginable without it. The general tendency towards more and more complex technical systems further pushes automated fault diagnosis applications and moves their systematic development into the focus of today’s system theoretical research.

1.1 Fault Diagnosis, Fault Detection and Isolation

Fault diagnosis is generally speaking *the activity of detecting, isolating, and identifying faults* that may possibly impact a system under investigation. These three intermediary tasks are generally described as follows (Blanke *et al.*, 2003):

- *Fault detection* determines whether some fault occurs. The effective fault remains however unknown.

- *Fault isolation* determines which particular fault affects the system. Hence an exact localization of the source of defect is required but not the determination of its particular magnitude.

- *Fault identification* estimates the magnitude of the fault affecting the system and determines the measure of damage.

Besides the diagnosis procedure itself, the term fault diagnosis also refers to the obtained diagnostic result.

Roughly speaking, fault diagnosis is executed by analyzing measured inputs and outputs of an investigated system (see Figure 1.1). Symptoms indicating the presence of specific faults are searched and subsequently interpreted in order to determine a correct and preferably unique fault diagnosis.

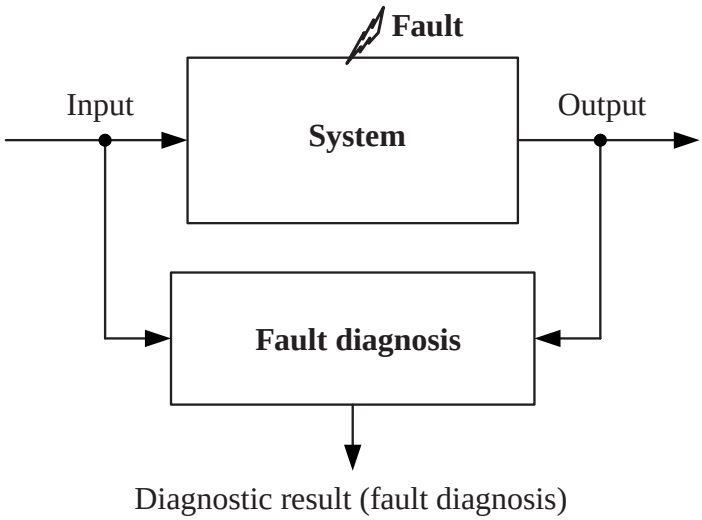


Figure 1.1: Schematic structure of fault diagnosis.

However, in the majority of diagnostic applications, the fault identification step is omitted and it is basically restricted to *fault detection and isolation (FDI)*. In general, FDI provides sufficient information for initiating fault responses like shutdown, reparation, or online-reconfiguration of the diagnosed system.

The focus of FDI can be basically assigned to the following three fields of diagnostic applications:

- *Monitoring (supervision).* System monitoring primarily focuses on safety critical processes like aircrafts, power plants, and chemical reactors. But it is also central in a variety of other application fields considering modern technical systems that have to be kept in a safe, environmentally compliant, and profitable operation. In order to provide decisive information for adequate fault reactions like dry-running operation or even shutdown, occurring faults have to be reliably detected as soon as possible. Additional fault isolation information usually

enables fault-specific reactions to be taken, hence may help to prevent unnecessary system failure. Whenever FDI functionalities are utilized for monitoring purposes, their online (real-time) computation is indispensable.

- *Fault finding.* In automated fault finding, FDI aims the serviceability of increasingly complex technical systems, that become more and more inscrutable. This is why automatic testers supporting the diagnosis process have become common practice in many fields of application, such as corrective maintenance in automotive and automation engineering. Of course, perceived real-system complexity almost always implies complex system representations which, in turn, complicate the design of automatic FDI algorithms. Because usually, increasing system complexity causes a growing number of potential fault candidates, particularly fault isolation becomes a challenging task. Unlike the monitoring task, this kind of FDI can be derived online, off-line, or in a combined on-/off-line approach; depending on the considered problem, the desired result, and the available computing equipment.

- *Fault-tolerant control.* The focus of fault tolerant control (FTC) is the maintenance of vital system functions, even in the faulty operation of a system. It is an important step towards the development of autonomously operating systems like robotics, unmanned aircraft, and aeronautic systems. The core of any FTC function is formed by an internal FDI algorithm that provides essential information for online-executed control system reconfiguration. FTC merges the classical fields of control system and FDI design and is one of the most promising fields of today's system theoretical research.

Automated FDI plays a central role in all of these different application fields. From a system theoretical point of view, indicators for real-world experienced complexity are e.g., system nonlinearity, multiple-input/multiple-output behavior, and high state dimension. The analysis and the design of FDI algorithms that are capable to deal with problems unifying these properties is a challenging task. The further development of existent FDI analysis and design methods that are capable of keeping step with the increasing complexity of modern technical systems is inevitable.

1.2 Research Directions of this Thesis

Motivated by the above discussion, this thesis is primarily concerned with the robust FDI of nonlinear systems in an uncertain discrete-time representation. The main research direction is the development of novel and computationally tractable analysis and synthesis methods for the FDI of uncertain nonlinear systems. In particular, this work considers systems of the form

$$\begin{aligned} x_{k+1} &= f\big(x_k, u_k, \delta_k, w_k\big),\ x_0,\ k \geq 0, \\ y_k &= h\big(x_k, u_k, \delta_k, v_k\big), \end{aligned}$$

or corresponding continuous-time formulations. Therein, x_k denotes the states, u_k the inputs, and y_k the outputs of the system. The system equations may depend on exogenous inputs w_k and v_k representing the influence of modeling uncertainties, disturbances, and measurement noise. Faults potentially affecting the system are described by the exogenous input δ_k which may enter both the system and the output equation. The class of FDI problems covered by the above model is large and not only includes a wide range of complex real-world systems like nonlinear and multiple-input/multiple-output systems but also a variety of different fault- and uncertainty-types. There is an abundance of examples in almost all application fields like electric drives, process technical plants, automobiles, aircrafts, and so on.

The field of robust FDI theory has reached a high level of maturity for the class of linear systems. Good introductions and overviews on linear FDI are given in (Blanke *et al.*, 2003) and (Ding, 2008) for example. The majority of the results in this area considers linear FDI approaches utilizing observers, parity relations, and parameter estimation methods. These methods have been successfully applied to many real-world problems both in academia and industry. However, in many practical applications, nonlinear systems have to be accomplished with and the use of nonlinear FDI methods is unavoidable. As discussed in more detail later on, there is a lack of robust FDI approaches for the above introduced nonlinear system class. On the one hand, there are quite few results with respect to diagnosability analysis; in particular in regard to more general classes of nonlinear systems. Nevertheless, applicable analysis tools are essential in order to check FDI problems for solvability and to get further insightful information enabling their successful FDI. On the other hand, the nonlinear FDI design itself is a largely open field, particularly in the case of uncertain nonlinear system representations. Another mainly open question is the treatment of intermittent and unanticipated faults. While intermittent faults result in a switching diagnosis environment that is difficult to handle, unanticipated faults cause unknown system operation making the system's observed behavior hard to be interpreted.

This work contributes to the solution of these open questions. Thereby it is particularly focused on the applicability and the computational tractability of the proposed analysis methods and the robust FDI algorithms respectively. Established results from continuous and hybrid observer theory form the foundation of the developed approach and are subsequently extended to FDI analysis and synthesis methods. The link between these fields, which would otherwise be different, is basically provided by a novel modeling formalism, that enables an efficient representation of a wide class of diagnosis problems. Further theoretical contributions are provided which complete this basis to a theoretically comprehensive approach to robust FDI. From a global point of view, this thesis gives a complete method to the robust FDI of nonlinear systems which is user oriented and applicable to a large class of practical FDI problems.

1.3 Thesis Outline and Contribution

The following overview displays an outline of this thesis and briefly summarizes its major contributions.

Chapter 2 – Nominal System, Uncertainty, and Fault Representation – formulates the basic problem setup and introduces the considered class of nonlinear systems, faults, and model uncertainties. In this context, a new system theoretical definition of the fault term is derived (Definition 2.1) according to DIN 40042 (Isermann, 1994). A practical DC actuator application example is introduced which serves as an illustration of further developments that follow in the subsequent chapters (Section 2.3).

Chapter 3 – Augmented State Models for FDI Analysis and Design - Nominal Case – provides a complete FDI design framework including modeling, analysis and FDI design for nonlinear diagnosis problems. Parts of this chapter are based on (Aßfalg and Allgöwer, 2006*b*) and (Aßfalg and Allgöwer, 2007).

- Structured augmented state model: A novel formalism for the representation of nonlinear systems subject to faults is introduced (Definition 3.1). The formulation is very general and allows the consideration of all fault types that are most commonly encountered in the FDI literature. By utilizing the well-known and practically approved principle of state augmentation, the FDI problem is moved close to the related field of nonlinear and hybrid (augmented) state estimation (Problem 3.1).

- Fault-detectability and -isolability conditions: New conditions for the fault-detectability and -isolability analysis of linear and nonlinear systems are introduced (Theorem 3.1 and Theorem 3.2). Both conditions employ the observability property in its fundamental notation of indistinguishable pairs of states, hence, they can be verified by utilizing established methods from observability analysis. The proposed conditions conceptually close the gap of practically applicable diagnosability analysis methods in the FID literature.

- FDI by hybrid augmented state estimation: FDI is suggested to be performed by means of approved hybrid state estimation techniques (Section 3.4).

Chapter 4 – Robust FDI with Uncertain Structured Augmented State Models – addresses the synthesis of robust FDI functions. Robustness of FDI is indispensable whenever the design engineer is obliged to rely on uncertain system and fault representations.

- Uncertain structured augmented state model: The structured augmented state modeling formalism is extended to a general class of uncertain nonlinear systems including uncertainties

of the system model, the fault representation, and unanticipated faults. Continuous uncertainties like disturbances, plant-model mismatch, and measurement noise are described by means of unknown-but-bounded uncertainty inputs which are intuitively and practically applicable. Unanticipated faults are captured in form of an unknown mode of operation enhancing the discrete part of the model.

- Robust FDI approach: After reviewing the background and introducing some basic notations of nonlinear set-valued estimation, a novel theoretical framework establishing the link to robust FDI is introduced. Starting off from the ideal solution to the nonlinear set-valued estimation problem, an ideal but computationally intractable approach to robust FDI is provided (Proposition 4.1 and Theorem 4.1). In the sequel, this is developed towards an approximate but practically computable solution (Proposition 4.2 and Theorem 4.2) which directly results in a simple robust FDI scheme for non-switching diagnosis problems.

- Robust fault-detectability and -isolability conditions: On the basis of the approximate approach, novel robust fault-detectability and -isolability conditions are derived (Proposition 4.3 and 4.4, Theorem 4.3 and 4.4). Provided that these conditions hold, a robust and non-trivial FDI can be determined by the suggested method.

- Robust FDI algorithm (switching case): Switching diagnosis environments resulting from intermittent faults and faults occurring/recovering within the FDI process are generally difficult to handle. In order to tackle this difficult class of problems, a novel robust FDI scheme is provided which is capable to diagnose both switching and non-switching problems (Algorithm 4.3).

Chapter 5 – Application to the Three-Tank Benchmark – presents an application of the proposed robust FDI synthesis approach. An example from chemical process diagnosis, namely the three-tank fault diagnosis problem, provides a concrete application that is well-studied in the literature. The example gives an insight into the application of the new results, i.e., of the proposed modeling formalism, the robust FDI algorithm and the selection of necessary tuning parameters.

Chapter 6 – Conclusions and Outlook – provides a summary of the thesis, discusses the achievements, and gives an outlook on possible further developments of the considered topics.

Chapter 2

Nominal System, Uncertainty, and Fault Representation

This chapter formulates the basic problem setup used throughout the remainder of this thesis. It introduces the classes of nonlinear systems, uncertainties and faults to be investigated and discusses their practical motivation. In the context of the proposed problem formulation, a system-theoretical definition of the fault term is derived from the current definition of fault as defined by DIN 40042. Most commonly differentiated fault types are explicated and shown to be contained in the described problem class. A practical example of a faulty operating DC actuator system is outlined which serves for illustrating the proposed setup and for attending the FDI considerations of the subsequent chapters.

2.1 Basic Problem Setup

Most physical systems are in fact continuous and nonlinear by nature. Their natural representation involves continuous-time nonlinear models which describe how the continuous states and outputs depend on the continuous initial state and (exogenous) input variables. However, the computing equipment which interacts with these physical systems, and on which FDI and also control algorithms are implemented, is digital. Such digital algorithms operate on discretized representations of the variables, hence require a discrete ”equivalent” model of the continuous system. Therefore discrete-time models describing the relationship among sampled variables of continuous systems have become widely established for representing continuous processes in automatic FDI and control (see for example (Gertler, 1998; Tyler *et al.*, 2000; Findeisen *et al.*, 2003; Rao *et al.*, 2003; Nguang *et al.*, 2007)). Other systems, mostly the ones existing on computers, are discrete by nature.

The thesis at hand deals with continuous- and discrete-time dynamic systems, where in general, nonlinear systems are investigated and linear ones are handled as special case. It is supposed

hereafter that the dynamics of the considered system can be described by an (uncertain) discrete-time model of the form

$$\Sigma : \begin{cases} x_{k+1} = f\big(x_k, u_k, \delta_k, w_k\big),\ x_0,\ k \geq 0, \\ \quad y_k = h\big(x_k, u_k, \delta_k, v_k\big), \end{cases} \tag{2.1}$$

where $x_k \in \mathbb{R}^{n_x}$ is the state vector of the system with initial value x_0, $u_k \in \mathbb{R}^{n_u}$ is the input vector, $y_k \in \mathbb{R}^{n_y}$ is the vector of measurements, and $\delta_k \in \mathbb{R}^{n_\delta}$ is an exogenous input vector representing the influence of possible faults (with positive integer k denoting the discrete-time index). Modeling uncertainties of the system and the output equation are captured by the exogenous inputs $w_k \in \mathbb{R}^{n_w}$ and $v_k \in \mathbb{R}^{n_v}$ respectively. The vector fields $f : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_\delta} \times \mathbb{R}^{n_w} \to \mathbb{R}^{n_x}$ and $h : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_\delta} \times \mathbb{R}^{n_v} \to \mathbb{R}^{n_y}$ represent the dynamics of the system.

Faults potentially affecting the system are considered in an exogenous input representation that has been proven to be very general and to be suited for describing all types of faults (Nyberg, 2003). In our further considerations, the exogenous fault input δ_k is considered to be a vectorial concatenation of N exogenous fault signals $\delta_k^{(i)} \in \mathbb{R}^{n_\delta^{(i)}}$, i.e.,

$$\delta_k = \big[\delta_k^{(1)T}, \ldots, \delta_k^{(N)T}\big]^T, \tag{2.2}$$

each characterizing an anticipated candidate for a potential fault $\mathcal{F}_i$. In further considerations, the following assumption holds regarding the possible occurrence of faults.

Assumption 2.1 *Any fault which potentially affects the system* (2.1) *comes forward as candidate of the* complete *set of N anticipated faults*

$$\mathbb{F} = \big\{\mathcal{F}_i,\ i \in \{1, \ldots, N\}\big\}. \tag{2.3}$$

Remark 2.1 *In general there is no possibility to prove whether a certain fault is present or not. This necessitates the assumption considering a fault as an element of a given fault set (see, e.g. (Blanke* et al.*, 2003)). The practical design of* (2.3) *would typically not only include previously experienced faults but also potential fault candidates that can be predicted from analyzing physically weak spots of a system. However, it is important to note that in practical applications, the completeness of the set* (2.3) *can never be assured, since it is impossible to exclude the occurrence of unforeseen faults. A robust FDI concept which allows to remedy this fundamental problem of modeling uncertainty in FDI will be provided in Chapter 4.*

The model uncertainties described by the exogenous inputs w_k and v_k, represent external disturbances, modeling errors as well as measurement noise. With respect to the uncertainty inputs w_k and v_k, it is assumed that both are *unknown-but-bounded*, i.e.,

$$w_k \in \mathbb{W}_k \subset \mathbb{R}^{n_w},\ v_k \in \mathbb{V}_k \subset \mathbb{R}^{n_v},\ \forall\, k \geq 0; \tag{2.4}$$

where $\mathbb{W}_k$ and $\mathbb{V}_k$ are compact (non-)uniform bounding sets of the uncertainty inputs w_k and v_k respectively.

Remark 2.2 *By allowing the sets $\mathbb{W}_k$ and $\mathbb{V}_k$ to be variant in time k, it is also possible to formulate nonuniform bounding sets $\mathbb{W}(x_k, u_k)$ and $\mathbb{V}(x_k, u_k)$ as functions of the system state x_k and the control input u_k. A simpler, though more restrictive assumption would be to assume that w_k and v_k are globally uniformly bounded, i.e., $w_k \in \mathbb{W}$ and $v_k \in \mathbb{V}$, $\forall\, k$, where $\mathbb{W}$ and $\mathbb{V}$ are constant sets. As an example, in many practical applications the nominal model is obtained by small-signal linearization techniques around a nominal operating point or trajectory. In this case $w_k = w(x_k, u_k)$ and $v_k = v(x_k, u_k)$ may represent the residual nonlinear terms, which are typically small for (x_k, u_k) close to the operating point but can be large elsewhere. In this case, imposing globally uniform bounds on w_k and v_k would be conservative and would decrease the achievable fault sensitivity. However, if nonuniform bounding sets are not known, the design engineer can consider the worst-case scenario and use uniform constant bounds as special cases.*

For the sake of well-posedness of problem (2.1), it is assumed that the states, the controls, and the fault inputs remain bounded for all times, i.e.,

$$x_k \in \mathbb{X} \subset \mathbb{R}^{n_x},\ u_k \in \mathbb{U} \subset \mathbb{R}^{n_u},\ \delta_k \in \mathbb{D} \subset \mathbb{R}^{n_\delta},\ \forall\, k \geq 0, \tag{2.5}$$

where $\mathbb{X}$, $\mathbb{U}$, and $\mathbb{D}$ are uniform compact bounding sets of the state, the control, and the fault input respectively.

Remark 2.3 *The reason for introducing the uniform bounding sets $\mathbb{X}$, $\mathbb{U}$, and $\mathbb{D}$ is just a formal one. In general, this work deals with the design and the analysis of fault detection and isolation schemes that are based on measurements of y_k and u_k. Since no fault accommodation is considered in this work, the (controlled or uncontrolled) system must be such that the measurable signals $y_k(x_k, u_k, \delta_k)$ remain bounded for all times, in other words, before and after the occurrence of a fault.*

Both faults and modeling uncertainties have been introduced as exogenous inputs acting on the system (2.1). Thus, from a system-theoretical point of view, there is no difference between uncertainties and faults. Their distinction is indeed subjective - we consider as faults those extra inputs the presence of which we wish to detect while we consider as uncertainty those which we want to ignore and be unaffected by. It remains to be seen in the subsequent chapters that the distinction between faults and uncertainties is, indeed, one of the crucial problems appearing in FDI practice.

2.2 Fault Term and Captured Fault-Types

So far, the concept of fault has been used rather intuitively. Even though anyone has a clear perception of a fault, the following considerations necessitate an exact system-theoretical characterization. By DIN 40042 a fault is defined as an *"incorrect deviation of at least one feature of a*

subject matter" (see e.g. (Isermann, 1994)). Applying this characterization to the exogenous fault input δ_k, which provides the above mentioned subject matter in further considerations, leads to the following definition of a fault.

Definition 2.1 *A fault $\mathcal{F}$ is defined as an incorrect deviation of the exogenous input δ_k from its fault-free (healthy) value $\delta_{\mathcal{H}}$, i.e.,*

$$\mathcal{F} : \delta_k \neq \delta_{\mathcal{H}}. \tag{2.6}$$

Thereby, $\delta_{\mathcal{H}} \in \mathbb{R}^{n_\delta}$ is a constant vector that is taken by δ_k in the fault-free operation of the system.

In the following, a brief survey of most commonly distinguished fault types is given. While Definition 2.1 gives an exact but also very general representation of faults, more specific characterizations as usually used in the FDI literature are investigated. Thereby, each of the subsequently introduced fault types is shown to be captured not only by the suggested problem formulation (2.1) but also by the above introduced definition of fault.

Input-, System-, and Output-Faults:

Depending on the position of the faults affecting a system, the differentiation between *input-faults*, *system-faults*, and *output-faults* has been proven to be useful in many practical FDI and FTC applications[1]. Associated discussions are found e.g. in the text-books (Gertler, 1998; Chen and Patton, 1999; Simani *et al.*, 2002; Blanke *et al.*, 2003). By exploiting the fault types' different actions in the input/output dynamics of a system, various methods for diagnosing specifically input- and output-faults have been established (see for example (Gertler, 1988; Li and Shah, 2002; Kwan and Xu, 2004; Mhaskar *et al.*, 2006)). In turn, there is a variety of approaches focusing on system faults only (Zhang *et al.*, 1999; Stoustrup and Niemann, 1999; Li and Jiang, 2004). Particularly with regard to the fault-specificity of these methodologies, this classification of faults has become indispensable in the FDI literature.

The system model (2.1) serves as basis for later FDI analysis and design steps. It is therefore fundamental that all of the above differentiated fault-types are included. In order to point out the generality of our problem formulation, the exogenous input δ_k is temporarily resolved into signals $\delta_k^{(u)}$, $\delta_k^{(x)}$, and $\delta_k^{(y)}$ characterizing input-faults, system-faults and output-faults respectively. Accordingly, the corresponding constants denoting the fault-free condition of (2.1) are divided into $\delta_{\mathcal{H}}^{(u)}$, $\delta_{\mathcal{H}}^{(x)}$, and $\delta_{\mathcal{H}}^{(y)}$. Under the terms of this classification, the system (2.1) can be partitioned into the input-sided sub-system

$$\Sigma_u : u'_k = g\big(u_k, \delta_k^{(u)}\big) \tag{2.7a}$$

[1] In the FDI/FTC literature it is usually distinguished between actuator-faults, system-faults, and sensor-faults, where system-faults mainly refer to parametric faults. Throughout this work, the synonyms of input-faults, system-faults, and output-faults are used instead. From a system theoretical point of view, these apply superiorly and more generally.

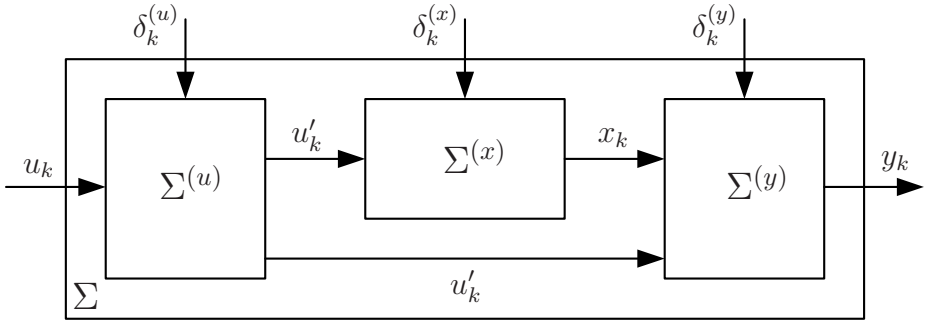


Figure 2.1: Input-, system-, and output faults and the corresponding partition of system (2.1) into subsystems specific to these fault types.

being subject to the exogenous input $\delta_k^{(u)}$, the central subsystem characterizing the system dynamics

$$\Sigma_x : x_{k+1} = f'\big(x_k, u'_k, \delta_k^{(x)}\big) \tag{2.7b}$$

affected by $\delta_k^{(x)}$, and the output-sided sub-system

$$\Sigma_y : y_k = h'\big(x_k, u'_k, \delta_k^{(y)}\big) \tag{2.7c}$$

underlying the influence of possible output-faults as modeled by $\delta_k^{(y)}$. Figure 2.1 visualizes the fault characteristics $\delta_k^{(u)}$, $\delta_k^{(x)}$, and $\delta_k^{(y)}$ dividing the system Σ into the sub-systems $\Sigma^{(u)}$, $\Sigma^{(x)}$, and $\Sigma^{(y)}$ respectively.

In the input-faulty operation, the signals u'_k effectively controlling the system (2.1) deviate from the expected control input u_k. The relation between u_k, $\delta_k^{(u)}$, and u'_k is given by the sub-system $\Sigma^{(u)}$. On the other hand, output faults cause differences between the measurements y_k and the real values to be measured (e.g. the states x_k), where x_k, u'_k, $\delta_k^{(y)}$, and y_k are related by the output function $\Sigma^{(y)}$. In the system-faulty case, undesirable modifications $\delta_k^{(x)}$ of the system dynamics $\Sigma^{(x)}$ (e.g. fault-conditioned parametric changes or modifications of the system equation) do occur.

In model (2.1), $f = f' \circ g$ and $h = h' \circ g$, where "$\circ$" denotes composition (for example $f' \circ g = f'(g)$). For brevity of exposition, further considerations re-use the compact formulation of (2.1), where differentiated expressions $\delta_k^{(u,x,y)}$ are abbreviated by δ_k, i.e., $\delta_{\mathcal{H}}^{(u,x,y)}$ by $\delta_{\mathcal{H}}$.

Additive and Multiplicative Faults:

Depending on the influence that occurring faults exert on the input, state and output variables of a system, the FDI literature commonly distinguishes between *additive* and *multiplicative faults* (Isermann, 1997; Gertler, 1998; Chen and Patton, 1999). To that effect, a variety of approaches concentrating either on additive or multiplicative fault detection and isolation have received significant attention in FDI literature (see for example (Stoustrup and Niemann, 2006; Garica and Frank, 1999; Ding *et al.*, 2003)). While in many cases the classification of a particular fault follows naturally from its nature, sometimes it may be also arbitrary. As an example, system-faults

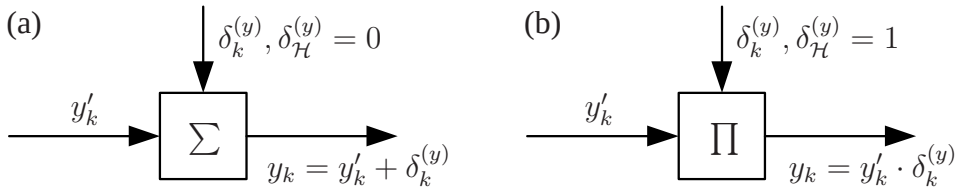


Figure 2.2: (a) Additive and (b) multiplicative formulation of an output-fault.

causing changes of plant parameters are always multiplicative, whereas input- and output-faults can be often expressed in both additive and multiplicative form. In contrast to multiplicative faults which usually introduce (additional) nonlinearity, additive faults are commonly simpler to deal with. Therefore, faults should be treated as additive whenever it can be reasonably justified. Figure 2.2 exemplifies the additive and the multiplicative formulation of an output-fault. In the additive representation of the exemplified output-fault (a), the fault-free case is characterized as $\delta_k^{(y)} := \delta_{\mathcal{H}}^{(y)} = 0$, whereas in the multiplicative case (b), one would have $\delta_k^{(y)} := \delta_{\mathcal{H}}^{(y)} = 1$.

As no additional assumptions are formulated regarding the way the exogenous input δ_k enters the system, the problem formulation (2.1) not only includes both additive and multiplicative faults but also treats them in the same manner.

Abrupt, Incipient, and Intermittent Faults:

In terms of the qualitative time dependent behavior of faults, it is basically distinguished between three types of faults in the FDI literature - *abrupt faults*, *incipient faults*, and *intermittent faults* (Gertler, 1998; Ballé, 2002) (see Figure 2.3). While, in general, abrupt faults affect the dynamics of a system drastically, the main difficulty in dealing with incipient faults is that their small effect on the system can already be hidden in minor modeling uncertainties. Intermittent faults usually occur abruptly and impact a system repetitively within short periods. Thus, their detection and isolation requires a continuous performance without respite.

Various fault-types most commonly differentiated in the FDI literature are investigated in this section and are shown to be captured by the problem setup described above as well as by the introduced definition of fault. Whereas most diagnosis methods stick to the FDI of such specific

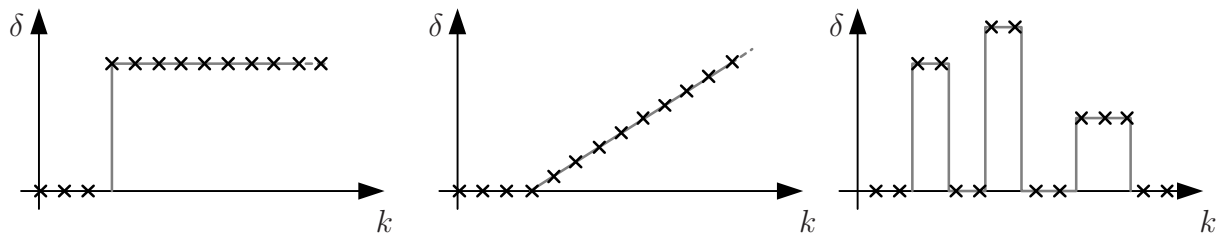


Figure 2.3: Variation in time of different fault types: (a) Abrupt fault, (b) incipient fault, and (c) intermittent fault.

types of faults, i.e., are limited to certain special cases of (2.1), it is our objective to develop FDI methodologies that enable the treatement of the general problem formulation. Before these developments are addressed in Chapters 3 and 4, the problem setup is illustrated by means of a practical example of a DC actuator system operating with faults.

2.3 Simple Example – DC Actuator System Subject to Faults

A simple DC actuator system is utilized as illustrative example of the above problem formulation (see Figure 2.4). This example will also play an important role in the following chapters. In certain subset configurations, it will serve for illustrating subsequently provided methods for FDI analysis and design.

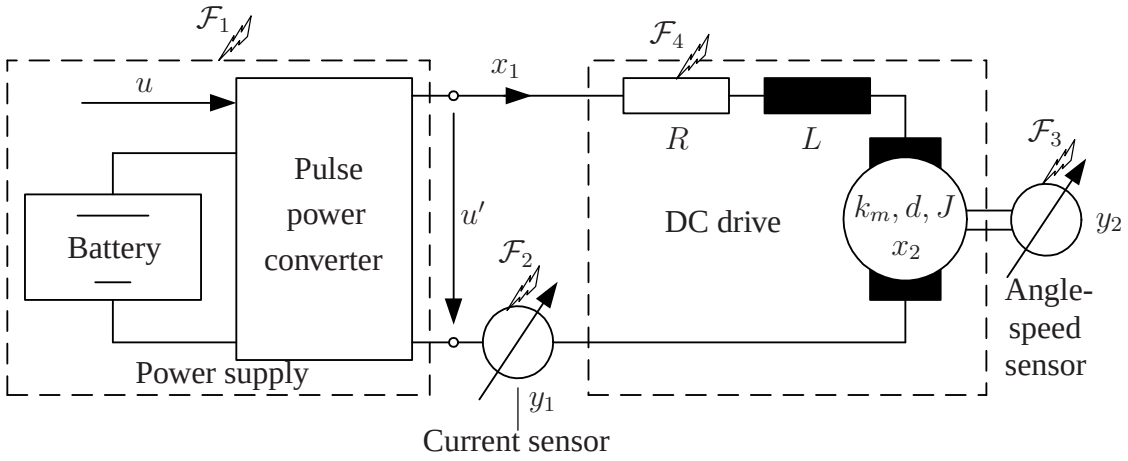


Figure 2.4: Schematic diagram of the exemplary DC actuator system which operates subject to the input-fault $\mathcal{F}_1$, the output-faults $\mathcal{F}_{2,3}$, and to the system-fault $\mathcal{F}_4$.

The DC actuator system basically consists of a power supply unit composed of a battery and a pulse power converter, an electrical DC drive, a current sensor, and an angle-speed sensor. The pulse power converter transforms the battery voltage into the voltage u' which effectively drives the actuator. In the fault-free condition, u' equals the preset supply voltage u (both in $[\mathrm{V}]$). Depending on the Ohmic resistor R and the inductive reactance L, the impressed voltage u' causes the electric current x_1 (in $[\mathrm{A}]$) to produce a magnetic torque being commensurate to the motor constant k_m. Depending on the motor inertia J and the viscous friction coefficient d, the motor-shaft rotates with the angle-speed x_2 (in $[\mathrm{rad/s}]$). Both the electric current and the angle-speed are measured by appropriate sensors providing the signals y_1 and y_2 respectively.

Using Kirchhoff's and Newton's law leads to the following continuous-time uncertain nonlinear model describing the dynamics of the DC actuator system:

$$\Sigma\colon \begin{cases} u'(t) = u(t) + \delta^{(1)}(t) \\ \dot{x}_1(t) = \dfrac{1}{L}\Big(-\big(R + \delta^{(4)}(t)\big)\, x_1(t) - k_m\, x_2(t) + u'(t)\Big) + w_1(t) \\ \dot{x}_2(t) = \dfrac{1}{J}\big(k_m\, x_1(t) - d\, x_2(t)\big) + w_2(t) \\ y_1(t) = x_1(t) + \delta^{(2)}(t) + v_1(t) \\ y_2(t) = x_2(t) + \delta^{(3)}(t) + v_2(t) \end{cases} , x(0) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{2.8}$$

Thereby $x(t) = [x_1(t)\ x_2(t)]^T$ is the state vector, $u(t)$ is the scalar control input, and $y(t) = [y_1(t)\ y_2(t)]^T$ is the vector of measurements, all at continuous-time t. The unknown but bounded uncertainty inputs $w(t) = [w_1(t)\ w_2(t)]^T$ and $v(t) = [v_1(t)\ v_2(t)]^T$ lump the plant-model-mismatch due to disturbances, modeling errors, parameter uncertainties and measurement noise. The physical parameters of the system are summarized in Table 2.1. For a more comprehensive review in respect of modeling DC drives, the interested reader is referred to e.g. (Leonhard, 2001).

Because both the control and the measurements are taken at discrete-time $t = k\,dT$ with a sampling rate $dT = 0.01$ [s], a discrete-time representation of (2.8) has to be deduced. Employing a simple Euler discretization

$$\dot{x}(t) \approx \frac{x_{k+1} - x_k}{dT} \tag{2.9}$$

leads to the following discrete-time uncertain nonlinear representation of the DC actuator system:

$$\Sigma\colon \begin{cases} u'_k = u_k + \delta_k^{(1)} \\ x_{1,k+1} = x_{1,k} + \dfrac{dT}{L}\big(-(R + \delta_k^{(4)})\, x_{1,k} - k_m\, x_{2,k} + u'_k\big) + w_{1,k} \\ x_{2,k+1} = x_{2,k} + \dfrac{dT}{J}\big(k_m\, x_{1,k} - d\, x_{2,k}\big) + w_{2,k} \\ y_{1,k} = x_{1,k} + \delta_k^{(2)} + v_{1,k} \\ y_{2,k} = x_{2,k} + \delta_k^{(3)} + v_{2,k} \end{cases} , x_0 = \begin{bmatrix} x_{1,0} \\ x_{2,0} \end{bmatrix}. \tag{2.10}$$

Thereby $x_k = [x_{1,k}\ x_{2,k}]^T$ is the discrete-time state vector, u_k is the scalar control input, and $y_k = [y_{1,k}\ y_{2,k}]^T$ is the vector of measurements taken at discrete-time $k\,dT$. The unknown-but-bounded uncertainty inputs $w_k = [w_{1,k}\ w_{2,k}]^T$ and $v_k = [v_{1,k}\ v_{2,k}]^T$ not only capture the modeling uncertainties $w(t)$ and $v(t)$ but also cover the additional uncertainty that is entailed with the approximation (2.9). The corresponding bounding sets are given as

$$\mathbb{W} : \Big\{ |w_{1,k}| \leq \bar{w}_1 = 0.1\,[\text{A}] \text{ and } |w_{2,k}| \leq \bar{w}_2 = 2.0\,[\text{rad/s}] \Big\} \tag{2.11a}$$

and

$$\mathbb{V} : \Big\{ |v_{1,k}| \leq \bar{v}_1 = 0.01\,[\text{A}] \text{ and } |v_{2,k}| \leq \bar{v}_2 = 0.02\,[\text{rad/s}] \Big\}, \tag{2.11b}$$

Table 2.1: Model parameter values of the DC actuator system.

Description	Symbol	Value	Unit
Motor constant	k_m	0.009	[Nm/A]
Inductive reactance	L	0.01	[H]
Ohmic resistance	R	0.443	[Ω]
Inertia	J	$2.0 \cdot 10^{-5}$	[kg/m^2]
Viscous friction coefficient	d	$5.5 \cdot 10^{-5}$	[Nm s/rad]
Sampling rate	dT	0.01	[s]

where $\bar{w}_1, \bar{w}_2$ and $\bar{v}_1, \bar{v}_2$ describe uniform upper bounds on the modeling uncertainties and the measurement noise respectively.

The fault input $\delta_k = [\delta_k^{(1)}\ \delta_k^{(2)}\ \delta_k^{(3)}\ \delta_k^{(4)}]^T$ lumps the effects of the anticipated faults $\mathcal{F}_1, \ldots, \mathcal{F}_4$. The anticipated faults $\mathcal{F}_1, \ldots, \mathcal{F}_4$ and the corresponding characteristics $\delta_k^{(1)}, \ldots, \delta_k^{(4)}$ are precisely specified as follows:

1. *Input-fault $\mathcal{F}_1$ (fault in power supply).* One additive input-fault affecting the power supply of the DC drive is considered. Due to this fault, the real impressed voltage $u'_k = u_k + \delta_k^{(1)}$ deviates by $\delta_k^{(1)}$ from the desired supply voltage u_k. In the fault-free case, we have $\delta_k^{(1)} := \delta_{\mathcal{H}}^{(1)} = 0$.

2. *Output-faults $\mathcal{F}_2$ and $\mathcal{F}_3$ (defective current and angle-speed sensor).* Due to these (additive) output faults, the measurements of the electric current and the angle-speed of the rotating motor-shaft deviate by $\delta_k^{(2)}$ and $\delta_k^{(3)}$ from the real values, i.e., $y_{1,k} = x_{1,k} + \delta_k^{(2)}$ and $y_{2,k} = x_{2,k} + \delta_k^{(3)}$. In the fault-free case, $\delta_k^{(2)} := \delta_{\mathcal{H}}^{(2)} = 0$ and $\delta_k^{(3)} := \delta_{\mathcal{H}}^{(3)} = 0$ hold.

3. *System-fault $\mathcal{F}_4$ (fault in the Ohmic resistor, e.g., due to coil overheating).* In the (multiplicative) system-faulty case, the Ohmic resistor deviates by $\delta_k^{(4)}$ from its fault-free value R. In the fault-free case, $\delta_k^{(4)} := \delta_{\mathcal{H}}^{(4)} = 0$.

Obviously the simplified block schematic of Figure 2.5 illustrates the exemplified system (2.10) completely and furthermore, is equivalent to the more complicated scheme as shown in Figure 2.4.

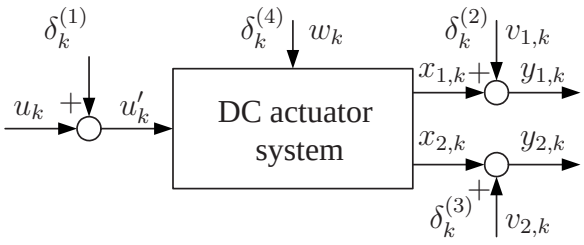


Figure 2.5: Simplified block schematic of the DC actuator system.

2.4 Summary

In this chapter, the basic setup for the subsequent FDI considerations is introduced. It represents a general class of uncertain discrete-time nonlinear systems subject to modeling uncertainties, to measurement noise, and to potential faults. Modeling uncertainties and measurement noise are described in a very practicable unknown-but-bounded exogenous input representation. Similarly, faults are modeled by (bounded) exogenous inputs, whereas no distinct bounding sets are supposed. Based on this fault representation, a system theoretical definition of the fault term is derived from the definition conforming to the standards of DIN 40042. Both the provided definition of fault and the corresponding model are shown to be very general and to include all types of faults as commonly encountered in the FDI literature.

The introduced setup is illustrated by means of a realistic example of a potentially faulty operating DC actuator system. In the remaining chapters, this will be used in different configurations in order to demonstrate the subsequent FDI analysis and design steps.

Chapter 3

Augmented State Models for FDI Analysis and Design – Nominal Case

This chapter introduces a new modeling formalism which is suitable to describe a general class of nonlinear FDI problems consistently. Conditions and practical procedures for linear and nonlinear fault-detectability and -isolability analysis are provided stating essential premises for the synthesis of FDI algorithms and filling a gap in the present FDI literature. Based on the suggested model, the fault diagnosis problem is specified as a hybrid augmented state estimation problem. Possible solutions to this problem are discussed and the FDI of a nominal configuration of the electrical DC actuator system of Section 2.3 is illustrated. As the considered problem class is large, the suggested approach is not only of theoretical interest but also of high practical relevance.

A prerequisite for investigations aiming towards a model-based FDI strategy is the rigorous dynamical modeling of the considered fault diagnosis problem. It provides the basis for the different conceptual stages of the FDI design procedure including fault-detectability and -isolability analysis as well as FDI algorithm design.

Indeed, the most distinctive characteristics between model-based FDI methods is the type of model used. The employed models not only differ in the representation of the based dynamical system but also vary in the representation of the potentially occuring fault candidates (see also Chapter 2). By this means, the most commonly encountered FDI approaches can be first of all divided in quantitative and qualitative methods. Quantitative methods can be basically classified in either linear approaches, like parity-space approaches (see, e.g. the references (Gertler and Singer, 1990; Gertler *et al.*, 1990)), (bi)linear observer-based approaches (Clark, 1979; Viswanadham and Srichander, 1987; Kinnaert, 1999), and parameter estimation approaches (Young, 1981; Isermann, 1989), and in nonlinear observer-based approaches (Frank, 1994; Hammouri *et al.*, 1999). The most common qualitative FDI methods are rule-based approaches (Ramesh *et al.*, 1992; Whiteley and Davis, 1992), petri net approaches (Ushio *et al.*, 2003), and state automaton approaches (Schröder, 2003).

An excellent overview and comparison of these different model types and the related FDI methods is given in the tripartite survey paper (Venkatasubramanian *et al.*, 2003*a*; Venkatasubramanian *et al.*, 2003*b*; Venkatasubramanian *et al.*, 2003*c*).

Whereas much research has been devoted to the design of FDI algorithms, rather few works investigate methods for fault-detectability and isolability analysis. Early works consider the detectability of jumps in linear systems (Caglayan, 1980) or consider detectability conditions in the frame of sensor selection problems (Tanaka, 1989). More recently, fault-detectability and -isolability conditions have been associated with specific FDI algorithms (Gertler and Singer, 1990; Nyberg and Nielsen, 2000). Considering the large number of established definitions, in (Staroswiecki and Darkhovski, 2001) a comparison between geometric and statistical fault-detectability/-isolability properties has been provided. Unlike the above cited references restricting to linear systems exclusively, in (Shumsky and Staroswiecki, 2003) the fault-detectability and -isolability analysis of nonlinear systems is investigated. Besides these quantitative approaches, the diagnosability of systems in the qualitative framework has been addressed by (Sampath *et al.*, 1995).

Although there have been a vast number of results on the modeling, analysis and diagnostic functionality design, there is presently no closed methodology that allows to accomplish these three conceptual stages in one common approach to a general class of practical FDI applications. This chapter presents a powerful approach to modeling in FDI and provides a complete development process including the analysis and the algorithm design for the single- and multiple-fault detection/isolation of a general class of nonlinear systems. The development starts off in Section 3.1 with a brief review of the underlying problem setup. In Section 3.2, the formalism of *structured augmented state models* is introduced which basically describes the possibly faulty operating system by a hybrid state automaton. In particular the practical results on fault-detectability and -isolability analysis of Section 3.3 conceptually close a gap in the FDI literature, since present analysis methods only treat some special cases and are difficult to evaluate even for simple diagnosis problems. The problem of FDI is specified as a hybrid augmented state estimation problem and possible solutions to the FDI design are approached in Section 3.4. The example of the faulty operating DC actuator system (see Section 2.3) finally illustrates the proposed method. Parts of this chapter are based on (Aßfalg and Allgöwer, 2006*b*; Aßfalg and Allgöwer, 2007).

3.1 Nominal Problem Setup

This chapter is devoted to nominal FDI problems abstracting away from disturbances and modeling uncertainties. According to this, the system to be diagnosed is described by the following nonlinear discrete-time model

$$\Sigma : \begin{cases} x_{k+1} = f\big(x_k, u_k, \delta_k\big),\ x_0,\ k \geq 0 \\ \quad y_k = h\big(x_k, u_k, \delta_k\big) \end{cases}, \tag{3.1}$$

where $x_k \in \mathbb{R}^{n_x}$ is the state vector of the system, $u_k \in \mathbb{R}^{n_u}$ is the input vector, $y_k \in \mathbb{R}^{n_y}$ is the vector of measurements, and $\delta_k \in \mathbb{R}^{n_\delta}$ is an exogenous input vector representing the influence of possible faults (with positive integer k denoting the discrete-time index). The vector fields $f : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_\delta} \to \mathbb{R}^{n_x}$ and $h : \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \times \mathbb{R}^{n_\delta} \to \mathbb{R}^{n_y}$ represent the dynamics of the system. The exogenous input vector δ_k is a vectorial concatenation (2.2) which satisfies the basic Assumption 2.1 (see Section 2.1).

3.2 Augmented State Modeling for FDI

As a preliminary step toward defining our virtual model, it shall be firstly glanced at the formalism of augmented state modeling (see also (Gelb *et al.*, 1974; Bar-Shalom and Li, 1993)). Forming the internal models of controllers and state estimators, augmented state models not only have proved to be suitable for tackling disturbances in system control and state estimation (Isidori *et al.*, 2004) but also for coping with challenging FDI problems (Liu and Liou, 1995; Lunze, 2003). Particularly for methodical purposes, the augmented state modeling approach demands attention since FDI can be accomplished by utilizing established (linear and nonlinear) state estimation methods. However, the drastically limited number of diagnosable faults has turned out to be a crucial shortcoming of this approach (Aßfalg and Allgöwer, 2006*b*). Hence, augmented state modeling will first of all provide a good basis which, however, will be enhanced in order to provide a modeling paradigm that is suitable for FDI - the structured augmented state model.

3.2.1 Fault Modeling by Exosystems

Up to now, the effects of faults have been treated as unrestricted arbitrary fault-signals. However, arbitrary fault signals are typically not plausible for technical reasons and provide only conservative fault models (Blanke, 1999). A common strategy to abate the conservativeness of this unknown input formulation, is to employ state augmentation. Thereby, the exogenous input signals δ_k are assumed to be generated by known dynamical exosystems that are concatenated with the nominal plant dynamics.

In the following, each fault signal $\delta_k^{(i)}$ is considered to be generated as the output of a stable dynamical exosystem

$$\Delta^{(i)} : \begin{cases} \xi_{k+1}^{(i)} = \phi^{(i)}\big(\xi_k^{(i)}\big),\ \xi_0^{(i)},\ k \geq 0 \\ \xi_{\mathcal{H}}^{(i)} = 0 \\ \delta_k^{(i)} = \psi^{(i)}\big(\xi_k^{(i)}, x_k, u_k\big) \\ \delta_{\mathcal{H}}^{(i)} = \text{const.} \end{cases}, \tag{3.2}$$

where $\phi^{(i)} : \mathbb{R}^{n_\xi^{(i)}} \to \mathbb{R}^{n_\xi^{(i)}}$ and $\psi^{(i)} : \mathbb{R}^{n_\xi^{(i)}} \times \mathbb{R}^{n_x} \times \mathbb{R}^{n_u} \to \mathbb{R}^{n_\delta^{(i)}}$ are sufficiently smooth vector functions of the fault-state $\xi_k^{(i)} \in \mathbb{R}^{n_\xi^{(i)}}$, the system state x_k, the control input u_k, and the fault characteristic $\delta_k^{(i)}$. In the fault-free condition, $\xi_k^{(i)} := \left(\xi_{\mathcal{H}}^{(i)} = 0\right)$ and $\delta_k^{(i)} := \left(\delta_{\mathcal{H}}^{(i)} = \text{const.}\right)$ hold by definition.

The exosystem (3.2) operates as a signal-generator whose nonlinear function $\phi^{(i)}$ and initial condition $\xi_0^{(i)}$ uniquely determine the fault-state $\xi_k^{(i)}$. Thus, with $\psi^{(i)}$, x_k, and u_k, the fault-signal $\delta_k^{(i)}$ is uniquely determined. The set $\mathbb{R}^{n_\xi^{(i)}}$ of admissible initial conditions and the exosystem $\Delta^{(i)}$ in conjunction specify a class of possible signals $\delta_k^{(i)}$. In this way, the so far unrestricted fault-signals $\delta_k^{(i)}$ get constrained to a smaller more realistic signal class.

Remark 3.1 *As discussed e.g. in (Gertler, 1988; Zhang* et al.*, 2002), many practical system-faults are nonlinear functions of the system state x_k and/or the control input u_k. For example, the outflow due to a leak in a pressure vessel is a nonlinear function of the interior pressure and the temperature. Such fault characteristics are captured in* (3.2) *by allowing the deviations $\delta_k^{(i)}$ to be nonlinear functions of the system state x_k and the input u_k. Other faults which can be modeled by* (3.2) *are, for instance, actuator-/sensor-faults, parametric faults, and system-faults causing the dynamics of* (3.1) *to change from $f(\cdot)$ to another nonlinear function. Thus, the fault model* (3.2) *is very general and allows to describe all types of faults that are relevant in practical FDI applications.*

Since in general, the nonlinear output-function $\psi^{(i)}$ is physically motivated, it is known in the majority of practical cases. In contrast, the dynamics of the exosystem (3.2) is rarely known in practice. This is why one normally has to rely on simple exosystem models expressing the expected class of signals $\xi_k^{(i)}$ sufficiently accurate. For this purpose, particularly linear exosystems have received significant attention in the control system and state estimation literature (see, e.g. (Cox, 1964; Isidori *et al.*, 2004)) as well as in diagnostic applications (Liu and Liou, 1995; Lunze, 2003). A tabular summary of several linear exosystems which can be used for exogenous input and fault representation is contained in (Gelb *et al.*, 1974).

Remark 3.2 *When time and frequency characteristics of an exogenous input are largely unknown, the assumption of piece-wise constant bias has proved to be very effective for a variety of applications (see, e.g. the references (Buja* et al.*, 1995; Aschemann* et al.*, 2000; Aßfalg* et al.*, 2006)). Due to the generally unpredictable nature of faults, such piece-wise constant approximations of the fault-states $\xi_k^{(i)}$ are due to be indispensable in most applications. In this case, the above introduced*

exosystem formulation reduces to

$$\Delta^{(i)}: \begin{cases} \xi_{k+1}^{(i)} = \xi_k^{(i)},\ \xi_0^{(i)},\ k \geq 0 \\ \xi_{\mathcal{H}}^{(i)} = 0 \\ \delta_k^{(i)} = \psi^{(i)}\big(\xi_k^{(i)}, x_k, u_k\big) \\ \delta_{\mathcal{H}}^{(i)} = \text{const.} \end{cases} \tag{3.3}$$

representing a special case of (3.2)*. To keep generality, further considerations in this thesis, nevertheless, are based on the general expression.*

3.2.2 Unstructured Augmented State Modeling

By using the fault model (3.2), the possible dynamics of system (3.1) originating from the fault $\mathcal{F}_i$ can be described by the augmented state model which is gained as the concatenation $\Sigma^{(i)} = \Sigma \circ \Delta^{(i)}$, i.e.,

$$\Sigma^{(i)}: \begin{cases} x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}, u_k\big),\ x_0^{(i)},\ k \geq 0 \\ y_k = h^{(i)}\big(x_k^{(i)}, u_k\big); \end{cases} \tag{3.4}$$

where $x_k^{(i)} = \big[x_k^T\ \xi_k^{(i)T}\big]^T \in \mathbb{R}^{n_x^{(i)}}$, $f^{(i)} = \big[(f \circ \psi^{(i)})^T\ \phi^{(i)T}\big]^T$, and $h^{(i)} = h \circ \psi^{(i)}$. However, as system (3.1) is subject to the set of potential fault-candidates $\mathbb{F}$, its possible dynamics (3.1) has to be described by an augmented state model that includes all N exosystems $\Delta^{(i)}$. This *unstructured augmented state model* is given by the concatenation $\Sigma^{(1,\ldots,N)} = \Sigma \circ \big(\Delta^{(1)}, \ldots, \Delta^{(N)}\big)$ which is determined as follows:

$$\Sigma^{(1,\ldots,N)}: \begin{cases} x_{k+1}^{(1,\ldots,N)} = f^{(1,\ldots,N)}\big(x_k^{(1,\ldots,N)}, u_k\big),\ x_0^{(1,\ldots,N)},\ k \geq 0 \\ y_k = h^{(1,\ldots,N)}\big(x_k^{(1,\ldots,N)}, u_k\big). \end{cases} \tag{3.5}$$

Thereby, the (unstructured) augmented state vector $x_k^{(1,\ldots,N)}$ is obtained by extending the system state vector x_k as

$$x_k^{(1,\ldots,N)} = \big[x_k^T\ \xi_k^{(1)T}, \ldots, \xi_k^{(N)T}\big]^T \in \mathbb{R}^{n_x^{(1,\ldots,N)}}, \tag{3.6}$$

where the according system equations $f^{(1,\ldots,N)}$ and $h^{(1,\ldots,N)}$ are formed by the following expressions:

$$f^{(1,\ldots,N)} = \big[(f \circ (\psi^{(1)}, \ldots, \psi^{(N)}))^T\ \phi^{(1)T}, \ldots, \phi^{(N)T}\big]^T,\ \ h^{(1,\ldots,N)} = h \circ \big(\psi^{(1)}, \ldots, \psi^{(N)}\big). \tag{3.7}$$

The unstructured augmented state model (3.5) gives a complete description of the potential faulty system (3.1) without containing an exogenous fault input anymore. From a methodical point of view, it is very useful: The FDI of system (3.1) can be accomplished by means of established methods for observing the augmented state $x_k^{(1,\ldots,N)}$ (Liu and Liou, 1995). Moreover, the diagnosability of (3.1) can be analyzed by verifying the observability of (3.5) (Lunze, 2003). This approach is

practically limited, which will now be illustrated by means of the DC actuator example introduced in Section 2.3. Thereby, for the sake of simplicity, the continuous-time representation (2.8) of the system and the faults is used temporarily.

Example 3.1 *Consider the continuous-time configuration of the electrical DC actuator system* (2.8) *and suppose that* $w(t), v(t) = 0$ *(nominal case). Furthermore suppose* (2.8) *to operate subject to the following set of three possible fault-candidates*

$$\mathbb{F} = \Big\{ \mathcal{F}_i, \Delta^{(i)} : \big\{ \dot{\xi}^{(i)}(t) = 0,\, \xi_0^{(i)},\, \delta^{(i)}(t) = \xi^{(i)}(t),\, \xi_{\mathcal{H}}^{(i)} = \delta_{\mathcal{H}}^{(i)} = 0 \big\},\; i \in [1,2,3] \Big\} \tag{3.8}$$

including the input-fault $\mathcal{F}_1$ *and the two output-faults* $\mathcal{F}_{2,3}$ *(see Section 2.3). Since the fault* $\mathcal{F}_4$ *remains unconsidered in this example, we have* $\delta_k^{(4)} := \delta_{\mathcal{H}}^{(4)} = 0$ *for all* k*. According to* (3.5)*, the unstructured augmented state model of the considered problem configuration is given as*

$$\Sigma^{(1,2,3)} : \begin{cases} \dot{x}^{(1,2,3)}(t) = \underbrace{\begin{bmatrix} -\frac{R}{L} & -\frac{c}{L} & \frac{1}{L} & 0 & 0 \\ \frac{c}{J} & -\frac{d}{J} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{A^{(1,2,3)}} x^{(1,2,3)}(t) + \underbrace{\begin{bmatrix} \frac{1}{L} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}}_{b^{(1,2,3)}} u(t) \\ y(t) = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}}_{C^{(1,2,3)}} x^{(1,2,3)}(t) \end{cases}, \tag{3.9}$$

where $x^{(1,2,3)}(t) = \big[x_1(t)\, x_2(t)\, \xi^{(1)}(t)\, \xi^{(2)}(t)\, \xi^{(3)}(t)\big]^T$ *denotes the augmented state vector. The actuator is controlled by the input* $u(t)$ *and observed by the measurements* $y(t)$*. Following (Lunze, 2003), the diagnosability of the considered problem can be analyzed by verifying the augmented state observability of* (3.9)*. Employing the linear Kalman rank criterion gives*

$$\operatorname{rank}\Big\{ \mathcal{O}\big(A^{(1,2,3)}, C^{(1,2,3)}\big) \Big\} \neq 5, \tag{3.10}$$

where $\mathcal{O}\big(A^{(1,2,3)}, C^{(1,2,3)}\big)$ *denotes the Kalman observability matrix (see, e.g. (Kailath, 1980)). Because matrix* (3.10) *has no full rank, the above exemplified problem of the faulty DC drive is thus not diagnosable in this setup.*

Remark 3.3 *Note that there are also criteria for checking the observability of discrete-time systems. Since these methods are not in the focus of this thesis, the exemplified observability analysis problems shall be restricted to the continuous-time case; which is also usual in the standard control systems literature. For a detailed discussion on observability of discrete-time systems, the interested reader is referred to, e.g., the references (Inouye, 1977; Aeyels, 1981; Nijmeijer, 1982).*

At first glance, the unstructured augmented state modeling approach to FDI proves to be advantageous as established methods for nonlinear state estimation and observability analysis can be utilized for (linear as well as nonlinear) FDI and diagnosability analysis. Nevertheless, as impressively demonstrated by Example 3.1, this approach is restricted to problems where only few faults are due; as a rough rule of thumb, the number of diagnosable faults equals the number of available measurement signals.

3.2.3 Structured Augmented-State Modeling

In real world FDI problems, potential faults rarely affect a system all at the same time. Hence, the unstructured problem formulation (3.5) is conservative in the majority of practical cases. The goal of this subsection is to provide a less conservative model that allows to overcome the limitations of the unstructured formalism.

3.2.3.1 Switched Fault Representation

In Definition 2.1, the fault term has been already introduced as an "incorrect" deviation of the exogenous input from its fault-free value $\delta_k \neq \delta_{\mathcal{H}}$, where $\delta_{\mathcal{H}}$ is a constant value being taken by δ_k in the fault-free condition of the system (3.1). So it is clear that the system operates faulty, if at least one element of the fault input δ_k is unequal to its fault-free value, i.e., if for at least one $i \in \{1, \ldots, N\}$, $\delta_k^{(i)} \neq \delta_{\mathcal{H}}^{(i)}$ holds (see also Section 2.1). As regards the occurrence of potential faults $\mathcal{F}_i : \delta_k^{(i)} \neq \delta_{\mathcal{H}}^{(i)}$, the following assumption holds throughout the remaining part of this work.

Assumption 3.1 *In the faulty operation of system* (3.1)*, only one potential fault (coming forward as candidate of the complete set $\mathbb{F}$) is allowed to be present at any time k. Consequently, the set $\mathbb{F}$ is specified as follows:*

$$\mathbb{F} = \left\{ \begin{array}{c} \mathcal{F}_1 : \delta_k = \left[(\delta_k^{(1)} \neq \delta_{\mathcal{H}}^{(1)})^T, \delta_{\mathcal{H}}^{(2)T}, \ldots, \delta_{\mathcal{H}}^{(N)T} \right]^T \\ \vdots \\ \mathcal{F}_N : \delta_k = \left[\delta_{\mathcal{H}}^{(1)T}, \delta_{\mathcal{H}}^{(2)T}, \ldots, (\delta_k^{(N)} \neq \delta_{\mathcal{H}}^{(N)})^T \right]^T \end{array} \right\}. \tag{3.11}$$

Remark 3.4 *By using the above assumption, the case in which system* (3.1) *operates subject to several fault candidates $\mathcal{F}_i$ simultaneously is ruled out. However, the possibility to consider multiple-faults is not excluded, since the fault characteristics $\delta_k^{(i)}$ may in turn represent concatenations of several single-fault characteristics.*

3.2.3.2 Structured Augmented State Model

In the following, an operating mode of system (3.1) is related to any fault $\mathcal{F}_i$ and to the fault-free case. The system is said to operate in the fault-free mode m_0, if $\delta_k = \delta_{\mathcal{H}}$. Contrary, if $\delta_k \neq \delta_{\mathcal{H}}$

results from an occurring fault $\mathcal{F}_i$, it is said to operate in the i-th faulty mode m_i. Extending the system equations (3.1) by the equations of the N exosystems (3.2) under the terms of the switched fault representation (2.3) yields $N+1$ augmented state models, each giving a complete description of the corresponding operating mode. According to this, the resulting set of $N+1$ operating modes is specified as follows:

$$\mathbb{Z} = \Big\{ m_0 : \Big\{ \Sigma^{(0)} := \Sigma\big(\delta_{\mathcal{H}}\big) \Big\},\ m_1 : \Big\{ \Sigma^{(1)} := \Sigma \circ \Delta^{(1)} \Big\},\ ...,\ m_N : \Big\{ \Sigma^{(N)} := \Sigma \circ \Delta^{(N)} \Big\} \Big\}. \quad (3.12)$$

It is important to note that

$$\mathbb{F} = \left\{ \begin{array}{c} \mathcal{F}_1 : \xi_k = \Big[(\xi_k^{(1)} \neq 0)^T, 0^T \Big]^T \\ \vdots \\ \mathcal{F}_N : \xi_k = \Big[0^T, (\xi_k^{(N)} \neq 0)^T \Big]^T \end{array} \right\} \quad (3.13)$$

is an equivalent representation of the fault set (2.3). Applying the equality constraints of (3.13) (and $\xi_k = 0^T$ in the fault-free mode) to the unstructured augmented state model (3.5) results in a switched $n_x^{(1,\ldots,N)}$-dimensional model that is equivalent to the model given by the above indicated tuple

$$\Big\{ \Sigma^{(i)},\ i \in \{0, \ldots, N\} \Big\}. \quad (3.14)$$

If each of the constraints (3.13) is re-formulated by means of $N+1$ mode-specific diagonal matrices $G_i^{n_x^{(1,\ldots,N)} \times n_x^{(1,\ldots,N)}}$ with elements $g_i \in \{0, 1\}$, each of the augmented models $\Sigma^{(i)}$ can be selected from (3.5) by switching the mode-specific equality constraint

$$G_i\, x_k^{(1,\ldots,N)} = 0 \ \Rightarrow\ x_k^{(i)} \in \mathbb{R}^{n_x^{(i)}}; \quad (3.15)$$

which forces mismatched fault-states to zero. From the perspective of this equivalent problem re-formulation, it becomes clear that by introducing the multiple-model representation (3.14), the unstructured augmented state space $\mathbb{R}^{n_x^{(1,\ldots,N)}}$ of (3.5) gets structured into subspaces $\mathbb{R}^{n_x^{(i)}}$ restricting possible augmented state trajectories mode-specifically (see Fig. 3.1). It remains to be seen in the next section that under certain conditions, a "gain of observability" is effected by imposing this structure.

Remark 3.5 *Note that the combination of the expressions* (3.5) *and* (3.15) *can be also particularly useful for an efficient implementation of the* $N+1$ *augmented state models contained in the tuple* (3.14). *Indeed the implementations of our subsequently introduced FDI algorithms employ this strategy. For the sake of simplicity, further considerations nevertheless use the notation of multiple-models* (3.14).

An important role in structuring the augmented state space $\mathbb{R}^{n_x^{(1,\ldots,N)}}$ is played by the rule type of switching between the operating modes m_i. As suggested in (Aßfalg and Allgöwer, 2006*b*), a

discrete-state automaton is employed that directly reflects an assumable fault scenario (the most commonly encountered is certainly a single-fault scenario (see Figure 3.2)). Thereby, the discrete-state automaton is described by the tuple

$$\mathcal{A}\big(\mathbb{Z}, \mathcal{G} : \mathbb{Z} \to \mathbb{Z}\big),\ z_0 \tag{3.16}$$

including the mode set $\mathbb{Z}$ with the related state variable $z_k \in \mathbb{Z}$, the discrete-state transition relation $\mathcal{G}$, and the initial discrete-state z_0. For comprehensive reviews of discrete-state automata, the interested reader is referred to the references (Cassandras and Lafortune, 1999; Lunze, 2003).

Remark 3.6 *Note that the structure of the discrete-state automaton* (3.16) *can be easily adapted to any arbitrary single- or multiple-fault scenario, e.g., to a scenario where a fault may occur, remain, and may cause another consecutive fault.*

Based on the tuple of augmented state models (3.14) and the discrete-state automaton (3.16), the structured augmented state model can be summarized as in the following definition.

Definition 3.1 (Structured augmented state model) *A structured augmented state model is described as a tuple*

$$\mathcal{S} := \Big\{\big\{\Sigma^{(i)},\ i \in \{0, \ldots, N\}\big\}, \mathcal{A}\Big\},\ x_0^{(i)}, z_0 \tag{3.17}$$

aggregating the $N + 1$ *mode-conditioned augmented state models* (3.4) *and the discrete-state automaton* (3.16)*.*

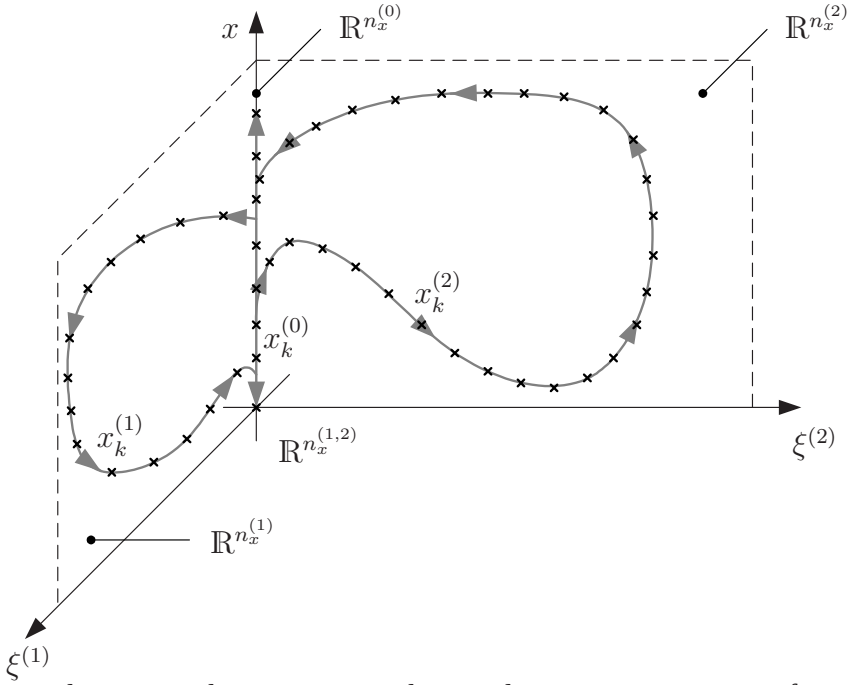


Figure 3.1: Structured augmented state space and exemplary state trajectories of an exemplary one-dimensional system operating subject to two single-faults $\mathcal{F}_1$ and $\mathcal{F}_2$ (each fault is described by a one-dimensional exosystem).

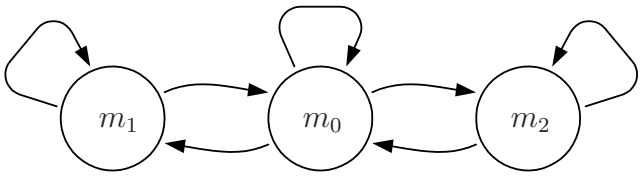


Figure 3.2: Mode transition graph of an example discrete-state automaton describing a classical single-fault scenario. The automaton contains three operating modes: The fault-free mode m_0 and the fault-modes $m_{1,2}$.

Figure 3.3 illustrates the construction of the structured augmented state model $\mathcal{S}$ with control input u_k and measured output y_k. The contained state automaton $\mathcal{A}$ is an autonomous discrete-event system that governs the switching between the mode-conditioned exosystems $\Delta^{(1)}, \ldots, \Delta^{(N)}$. In the fault-free mode $z_k = m_0$, the fault-states $\xi_k^{(1)}, \ldots, \xi_k^{(N)}$ are constrained to zero, i.e., in the i-th fault-mode $z_k = m_i$, the mismatched fault-states. Accordingly, the fault-characteristics $\delta_k^{(i)}$ take their fault-free values $\delta_{\mathcal{H}}^{(i)}$ since $\psi^{(i)}\big(\xi_k^{(i)} = 0, \cdot\big) := \delta_{\mathcal{H}}^{(i)}$.

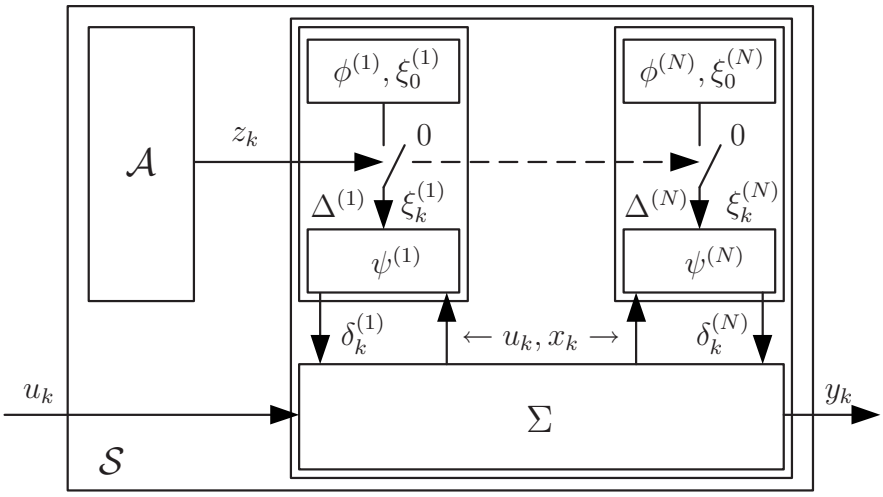


Figure 3.3: Block diagram of the structured augmented state model.

3.3 Properties of the Structured Augmented System

The introduction of the structured augmented state model is motivated by the objective to overcome the diagnosability limitations of the unstructured approach (see Example 3.1). Let us now attend to the fault-detectability and –isolability properties of systems that can be described by means of the structured problem representation. The afore highlighted relationship between augmented state observability analysis and diagnosability analysis will be exploited and enhanced to the structured formalism. Before this is turned to, let us first introduce a basic definition of the observability property as given in e.g. (Nijmeijer and Van der Schaft, 1990).

Definition 3.2 *Two states $x_0^*, x_0^{**} \in \mathbb{R}^n$, $x_0^* \neq x_0^{**}$ are said to be indistinguishable (denoted $x_0^* I x_0^{**}$) for a system*

$$\begin{aligned} x_{k+1} &= f\big(x_k, u_k\big),\ x_0,\ k \geq 0 \\ y_k &= h\big(x_k, u_k\big), \end{aligned} \tag{3.18}$$

if for every admissible input function u_k, the output function $y_k(x_0^*, u_k)$[1] for the system with initial state x_0^*, and the output function $y_k(x_0^{**}, u_k)$ for the system with initial state x_0^{**}, are identical on their common domain of definition. The system (3.18) *is called observable, if $x_0^* I x_0^{**}$ implies $x_0^* = x_0^{**}$ for all admissible input functions u_k.*

Mathematical conditions for verifying the observability of systems (3.18) by virtue of Definition 3.2 have been extensively discussed by various authors. In this respect, the interested reader is directed to e.g. (Kou *et al.*, 1973; Hermann and Krener, 1977; Nijmeijer and Van der Schaft, 1990).

Using again the idea of indistinguishable pairs of states that is already used in Definition 3.2, the structured augmented system properties of fault-detectability and -isolability can be specified as follows.

Definition 3.3 (Fault-detectability and -isolability) *Two modes $(m_i \neq m_j) \in \mathbb{Z}$ are said to be* indistinguishable *(denoted $m_i \, I \, m_j$) for* (3.17)*, if for every admissible input function u_k, the output function $y_k(m_i, u_k)$ for the structured augmented system operating in mode $z_k = m_i$, and the output function $y_k(m_j, u_k)$ for the structured augmented system operating in mode $z_k = m_j$, are identical on their common domain of definition. The structured augmented system* (3.17) *is called* fault-detectable*, if, for all pairs $(i = 0, j \in \{1, \ldots, N\})$, $m_i \, I \, m_j$ implies $m_i = m_j$; and is called* fault-isolable*, if, for all pairs $(i \neq j) \in \{0, \ldots, N\}$, $m_i \, I \, m_j$ implies $m_i = m_j$.*

Starting from Definition 3.3 and Definition 3.2, which is based on the most commonly used notion of indistinguishable pairs of states, a general condition for the distinguishabilty of two operating modes $(m_i \neq m_j) \in \mathbb{Z}$ can be stated (Aßfalg and Allgöwer, 2006*b*).

Proposition 3.1 *Consider the two operating modes $(m_i \neq m_j) \in \mathbb{Z}$ of the structured augmented system* (3.17)*. The modes m_i and m_j are distinguishable, if the augmented system*

$$\Sigma^{(i,j)} : \begin{cases} x_{k+1}^{(i,j)} = f^{(i,j)}\big(x_k^{(i,j)}, u_k\big), x_0^{(i,j)},\ k \geq 0 \\ \quad y_k = h^{(i,j)}\big(x_k^{(i,j)}, u_k\big) \end{cases} \tag{3.19}$$

is observable in terms of Definition 3.2; where $f^{(i,j)} = \big[(f \circ (\psi^{(i)}, \psi^{(j)}))^T \ \phi^{(i)T} \ \phi^{(j)T}\big]^T$, $h^{(i,j)} = h \circ (\psi^{(i)}, \psi^{(j)})$, and $x_k^{(i,j)} = \big[x_k^T \ \xi_k^{(i)T} \ \xi_k^{(j)T}\big]^T$.

[1] In observability analysis for dynamical systems, an important role is played not only by the dependency of y on the time k, but also by its dependency on the initial state x_0 and the input u. Therefore, Definition 3.2 avails the notation $y_k(x_0, u)$ instead of y_k.

Proof. First note that the ability to distinguish between *any* pair $x_0^{(i,j)*}$, $x_0^{(i,j)**}$ on the basis of the observations $y_k\big(x_0^{(i,j)*}, u_k\big)$ and $y_k\big(x_0^{(i,j)**}, u_k\big)$ (denoted $x_0^{(i,j)*} D\, x_0^{(i,j)**}$) is implied by the observability of (3.19) (see Definition 3.2). As $x_0^{(i,j)}$ includes both $x_0^{(i)}$ and $x_0^{(j)}$ as special cases, the distinguishability of the two augmented states $x_0^{(i)}$, $x_0^{(j)}$ is guaranteed, i.e.,

$$\left\{\left(x_0^{(i,j)*} = \begin{bmatrix} x_0^* \\ \xi_0^{(i,j)*} \end{bmatrix}\right) := \left(x_0^{(i)} = \begin{bmatrix} x_0 \\ \xi_0^{(i)} \\ 0 \end{bmatrix}\right)\right\} D \left\{\left(x_0^{(ij)**} = \begin{bmatrix} x_0^{**} \\ \xi_0^{(i,j)**} \end{bmatrix}\right) := \left(x_0^{(j)} = \begin{bmatrix} x_0 \\ 0 \\ \xi_0^{(j)} \end{bmatrix}\right)\right\}.$$

The only exception is $x_0^{(i)}\, I\, x_0^{(j)}$, if $x_0^{(i)} = x_0^{(j)}$ - which is only the case in the fault-free operation being captured by the definition of the mode m_0. As $y_k\big(x_0^{(i,j)*} := x_0^{(i)}, u_k\big) \equiv y_k(m_i, u_k)$ and $y_k\big(x_0^{(i,j)**} := x_0^{(j)}, u_k\big) \equiv y_k(m_j, u_k)$, we have $m_i\, D\, m_j$. ∎

Applying the results of Proposition 3.1, the following condition for the fault-detectability of (3.17) can be given (Aßfalg and Allgöwer, 2006*b*).

Theorem 3.1 (Fault-detectability condition) *The structured augmented system* (3.17) *is* fault-detectable*, if, for all* $i \in \{1, \ldots, N\}$*, the augmented systems*

$$\Sigma^{(i)} : \begin{cases} x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}, u_k\big), x_0^{(i)},\ k \geq 0 \\ \quad y_k = h^{(i)}\big(x_k^{(i)}, u_k\big) \end{cases} \tag{3.20}$$

are observable in terms of Definition 3.2; where $f^{(i)} = \big[(f \circ \psi^{(i)})^T\ \phi^{(i)T}\big]^T$, $h^{(i)} = h \circ \psi^{(i)}$, *and* $x_k^{(i)} = \big[x_k^T\ \xi_k^{(i)T}\big]^T$.

Proof. The proof of Theorem 3.1 directly follows from the combination of Definition 3.3 and Proposition 3.1. ∎

Similar to the fault-detectability condition, a condition for verifying the fault-isolability of the system (3.17) can be stated (Aßfalg and Allgöwer, 2006*b*).

Theorem 3.2 (Fault-isolability condition) *Consider the structured augmented system* (3.17) *and suppose that the fault-detectability condition (Theorem 3.1) is satisfied. Then,* (3.17) *is* fault-isolable*, if, for all pairs* $(i \neq j) \in \{1, \ldots, N\}$*, the augmented systems*

$$\Sigma^{(i,j)} : \begin{cases} x_{k+1}^{(i,j)} = f^{(i,j)}\big(x_k^{(i,j)}, u_k\big), x_0^{(i,j)},\ k \geq 0 \\ \quad y_k = h^{(i,j)}\big(x_k^{(i,j)}, u_k\big) \end{cases} \tag{3.21}$$

are observable in terms of Definition 3.2; where $f^{(i,j)} = \big[(f \circ (\psi^{(i)}, \psi^{(j)}))^T\ \phi^{(i)T}\ \phi^{(j)T}\big]^T$, $h^{(i,j)} = h \circ (\psi^{(i)}, \psi^{(j)})$, *and* $x_k^{(i,j)} = \big[x_k^T\ \xi_k^{(i)T}\ \xi_k^{(j)T}\big]^T$.

Proof. Similar to the previous theorem, the proof of Theorem 3.2 also follows from combining Definition 3.3 and Proposition 3.1. ∎

Remark 3.7 *Note that neither Theorem 3.1 nor Theorem 3.2 explicitly use the index $i = 0$ identifying the fault-free mode m_0. Of course, the fault-free mode is considered by both conditions anyhow. In Theorem 3.1, the augmented expression $\Sigma^{(i)} = \Sigma \circ \Delta^{(i)}$ could be also denoted as $\Sigma^{(0i)}$.*

Fault-detectability and -isolability have been introduced as properties of the structured augmented system (3.17). This makes sense, the more so as these properties depend not only on the character of the dynamics Σ, the available measurements y_k, and the control inputs u_k but also on the number N of possible faults $\mathcal{F}_i$, their constitution $\Delta^{(i)}$, and the satisfied scenario $\mathcal{A}$. According to this, the properties of fault-detectability and -isolability refer to the real system as well as to the (fictive) dynamics of possible faulty operating modes.

Theorems 3.1 and 3.2 give conditions for verifying the fault-detectability/-isolability of FDI problems (3.17). From a practical point of view, both conditions are of particular interest since they can be verified by utilizing established methods for linear and nonlinear observability analysis. Since both theorems are proven by using the fundamental notion of indistinguishable pairs of states, they can be applied to both continuous- and discrete-time systems by choosing the corresponding observability analysis method. The above conditions are much more general and, in addition, easier to apply than common fault-detectability and -isolability analysis methods. Hence, Theorem 3.1 and 3.2 constitute an improvement in comparison to present FDI literature. In order to establish a better understanding, a further example investigating the DC actuator system is presented. This illustrates the main result of this section and outlines the convenience of the proposed analysis methods.

Example 3.2 *Consider the problem configuration as already used in Example 3.1. However, suppose now a classical single-fault scenario to hold. Then, the corresponding structured augmented state model is basically described by the tuple*

$$\Sigma^{(1)} \quad : \quad \begin{cases} \dot{x}^{(1)}(t) = \underbrace{\begin{bmatrix} -\frac{R}{L} & -\frac{c}{L} & \frac{1}{L} \\ \frac{c}{J} & -\frac{d}{J} & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{A^{(1)}} x^{(1)}(t) + \underbrace{\begin{bmatrix} \frac{1}{L} \\ 0 \\ 0 \end{bmatrix}}_{b^{(1)}} u(t) \\ y(t) = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}}_{C^{(1)}} x^{(1)}(t), \end{cases} \tag{3.22a}$$

$$\vdots$$

$$\Sigma^{(3)} \quad : \quad \begin{cases} \dot{x}^{(3)}(t) = \underbrace{\begin{bmatrix} -\frac{R}{L} & -\frac{c}{L} & 0 \\ \frac{c}{J} & -\frac{d}{J} & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{A^{(3)}} x^{(3)}(t) + \underbrace{\begin{bmatrix} \frac{1}{L} \\ 0 \\ 0 \end{bmatrix}}_{b^{(3)}} u(t) \\ y(t) = \underbrace{\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}}_{C^{(3)}} x^{(3)}(t), \end{cases} \tag{3.22b}$$

where $x^{(1)}(t) = \left[x_1(t)\, x_2(t)\, \xi^{(1)}(t)\right]^T, \ldots, x^{(3)}(t) = \left[x_1(t)\, x_2(t)\, \xi^{(3)}(t)\right]^T$*. According to Theorem 3.1, the fault-detectability of the considered problem can be verified by employing three times the linear Kalman rank criterion as*

$$\text{rank}\Big\{\mathcal{O}\big(A^{(1)}, C^{(1)}\big)\Big\} = 3, \text{rank}\Big\{\mathcal{O}\big(A^{(2)}, C^{(2)}\big)\Big\} = 3, \text{rank}\Big\{\mathcal{O}\big(A^{(3)}, C^{(3)}\big)\Big\} = 3, \tag{3.23}$$

where $\mathcal{O}\big(A^{(i)}, C^{(i)}\big)$ *denote the Kalman observability matrices of the augmented systems* $\Sigma^{(i)}$*. Because each of the observability matrices has full rank, the exemplified single-fault scenario is fault-detectable in virtue of Theorem 3.1.*

According to Theorem 3.2, the fault-isolability can be checked similarly by verifying the observability of the augmented systems $\Sigma^{(1,2)}$*,* $\Sigma^{(1,3)}$*, and* $\Sigma^{(2,3)}$*, i.e., of*

$$\Sigma^{(1,2)} \quad : \quad \begin{cases} \dot{x}^{(1,2)}(t) = \underbrace{\begin{bmatrix} -\frac{R}{L} & -\frac{c}{L} & \frac{1}{L} & 0 \\ \frac{c}{J} & -\frac{d}{J} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{A^{(1,2)}} x^{(1,2)}(t) + \underbrace{\begin{bmatrix} \frac{1}{L} \\ 0 \\ 0 \\ 0 \end{bmatrix}}_{b^{(1,2)}} u(t) \\ y(t) = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}}_{C^{(1,2)}} x^{(1,2)}(t), \end{cases} \tag{3.24a}$$

$$\vdots$$

$$\Sigma^{(2,3)} \quad : \quad \begin{cases} \dot{x}^{(2,3)}(t) = \underbrace{\begin{bmatrix} -\frac{R}{L} & -\frac{c}{L} & 0 & 0 \\ \frac{c}{J} & -\frac{d}{J} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{A^{(2,3)}} x^{(2,3)}(t) + \underbrace{\begin{bmatrix} \frac{1}{L} \\ 0 \\ 0 \\ 0 \end{bmatrix}}_{b^{(2,3)}} u(t) \\ y(t) = \underbrace{\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}}_{C^{(2,3)}} x^{(2,3)}(t); \end{cases} \tag{3.24b}$$

where $x^{(1,2)}(t) = \left[x_1(t)\, x_2(t)\, \xi^{(1)}(t)\, \xi^{(2)}(t)\right]^T, \ldots, x^{(2,3)}(t) = \left[x_1(t)\, x_2(t)\, \xi^{(2)}(t)\, \xi^{(3)}(t)\right]^T$. *Employing the linear Kalman rank criterion as*

$$\text{rank}\Big\{\mathcal{O}\big(A^{(1,2)}, C^{(1,2)}\big)\Big\} = 4, \text{rank}\Big\{\mathcal{O}\big(A^{(1,3)}, C^{(1,3)}\big)\Big\} = 4, \text{rank}\Big\{\mathcal{O}\big(A^{(2,3)}, C^{(2,3)}\big)\Big\} = 4, \quad (3.25)$$

with $\mathcal{O}\big(A^{(i,j)}, C^{(i,j)}\big)$ *denoting the Kalman observability matrices of the augmented systems* $\Sigma^{(i,j)}$*, verifies the distinguishability of the modes* $m_1\, D\, m_2$*,* $m_1\, D\, m_3$*, and* $m_2\, D\, m_3$*. Hence, combined with the precedent fault-detectability analysis, the fault-isolability of the DC drive is verified according to Theorem 3.2.*

By means of a linear configuration of the DC actuator example, the application of Theorem 3.1 and Theorem 3.2 has been illustrated. It has been shown that in the linear (continuous-time) case, both theorems can be easily verified by utilizing the linear Kalman rank criterion. Expectedly in the nonlinear case, fault-detectability and -isolability analysis turn out to be more complicated and different forms of fault-detectability and -isolability have to be considered. With respect to the relationship between the results of the Theorem 3.1 and Theorem 3.2 and observability analysis, it lends itself to introduce (in analogy to the known definitions of nonlinear observability, see e.g. the literature (Hermann and Krener, 1977; Birk, 1992)) the practical forms of *global*, *local*, and *operating point fault-detectability and -isolability*. These properties are specified in the following definition.

Definition 3.4 (Fault-detectability/-isolability forms) *The structured augmented system* (3.17) *is called*

- *globally fault-detectable, if, for all* $i \in \{1, \ldots, N\}$ *and for all* $u_k \in \mathbb{R}^{n_u}$*, the initial augmented states* $x_0^{(i)}$ *are uniquely determinable from* (u_k, y_k) *in the whole domain of definition* $x_0^{(i)} \in \mathbb{R}^{n_x^{(i)}}$*,*

- *locally fault-detectable in a point* $x_P^{(i)}$*, if, for all* $i \in \{1, \ldots, N\}$ *and for all* $u_k \in \mathbb{R}^{n_u}$*, the initial augmented states* $x_0^{(i)}$ *are uniquely determinable from* (u_k, y_k) *in a neighborhood* $||x_0^{(i)} - x_P^{(i)}|| < \rho_P$ *of* $x_P^{(i)}$*; the system is locally fault-detectable if this property holds for all points* $x_P^{(i)} \in \mathbb{R}^{n_x^{(i)}}$*,*

- *fault-detectable in an operating point* $x_S^{(i)}$*, if, for all* $i \in \{1, \ldots, N\}$*, the initial augmented states* $x_0^{(i)}$ *are uniquely determinable from* (u_k, y_k) *in a neighborhood* $||x_0^{(i)} - x_S^{(i)}|| < \rho_{S_x}$*,* $||u - u_S|| < \rho_{S_u}$ *of the equilibrium* $x_S^{(i)}$*,* u_S*.*

The structured augmented system is called globally fault-isolable, locally fault-isolable in a point $x_P^{(i,j)}$*, locally fault-isolable, and fault-isolable in an operating point* $x_S^{(i,j)}$*, if these properties hold for all pairs* $i \neq j \in \{1, \ldots, N\}$ *concerning the augmented initial state* $x_0^{(i,j)}$*.*

Similar to observability analysis, in FDI, the analysis of nonlinear systems necessitates a discrimination between different fault-detectability and -isolability forms. Opposed to the linear case, these properties may also depend on the control-input u_k and, in general, do not hold globally a priori. In practical FDI applications, such characteristic behavior of nonlinear systems often becomes noticeable in that for a successful FDI, a certain (persistent) excitation forcing a certain operation of the system is required. The following example investigates the fault-detectability and -isolability analysis for the nonlinear configuration of the DC actuator example.

Example 3.3 *Consider again the continuous-time configuration of the electrical DC actuator system* (2.8) *and suppose that* $w(t), v(t) = 0$ *(nominal case). Suppose* (2.8) *to operate subject to the complete set of four possible fault-candidates satisfying a single-fault scenario: The input-fault* $\mathcal{F}_1$*, the two output-faults* $\mathcal{F}_{2,3}$*, and the system-fault* $\mathcal{F}_4$ *(see Section 2.3). Using again a constant-type fault representation, the set of possible faults can be described as*

$$\mathbb{F} = \Big\{ \mathcal{F}_i, \Delta^{(i)} : \big\{ \dot{\xi}^{(i)}(t) = 0,\, \xi_0^{(i)},\, \delta^{(i)}(t) = \xi^{(i)}(t),\, \xi_{\mathcal{H}}^{(i)} = \delta_{\mathcal{H}}^{(i)} = 0 \big\},\, i \in \{1, \ldots, 4\} \Big\}. \tag{3.26}$$

Based on the single-fault assumption, the structured augmented state model is basically given by the tuple $\Sigma^{(1)}, \ldots, \Sigma^{(4)}$ *containing the linear expressions* $\Sigma^{(1)}$*,* $\Sigma^{(2)}$*,* $\Sigma^{(3)}$ *(as already derived in Example 3.2) and the nonlinear expression*

$$\Sigma^{(4)} : \begin{cases} \dot{x}^{(4)}(t) = \begin{bmatrix} \frac{1}{L}\big(u(t) - \big(R + x_3^{(4)}(t)\big)x_1^{(4)}(t) - c x_2^{(4)}(t)\big) \\ \frac{1}{J}\big(c x_1^{(4)}(t) - d x_2^{(4)}(t)\big) \\ 0 \end{bmatrix}; \\ \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix} = \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} \end{cases} \tag{3.27}$$

with $x^{(4)}(t) = \big[x_1(t)\, x_2(t)\, \xi^{(4)}(t)\big]^T$*. In order to verify the fault-detectability of the considered problem under the terms of Theorem 3.1, the observability of* $\Sigma^{(4)}$ *has to be checked. Following e.g. (Birk, 1992), this can be verified locally as*

$$\mathit{rank}\Big\{ \mathcal{O}\big(\Sigma^{(4)}\big) \Big\} = 3,\, \forall\, u(t),\, \forall\, x_P^{(4)} \in \mathbb{R}^{n_x^{(4)}}, \tag{3.28}$$

where $\mathcal{O}\big(\Sigma^{(4)}\big)$ *denotes the local observability matrix* [2] *depending on the augmented state* $x^{(4)}(t)$*, the input* $u(t)$*, and the* $n_x^{(4)} - 1$ *derivatives of* $u(t)$*:*

$$\mathcal{O}\big(\Sigma^{(4)}\big) = \left. \frac{\partial q^{(4)}}{\partial x^{(4)}(t)} \right|_{x^{(4)}(t) = x_P^{(4)}},\; x^{(4)}(t) = {q^{(4)}}^{-1}\left({}^{[n_x^{(4)}-1]}y(t),\, {}^{[n_x^{(4)}-1]}u(t) \right). \tag{3.29}$$

[2] The local observability matrices used for the fault-detectability and -isolability analysis of this example, have been determined with the *Symbolic-Math Toolbox of MatLab.* Even for this simple example, the analytical expressions of the local observability matrices get large. This is why, for the sake of brevity, a detailed consideration of the involved local nonlinear observability analysis steps has been omitted. For a comprehensive review on nonlinear observability analysis, the reader is referred to e.g. (Nijmeijer and Van der Schaft, 1990; Birk, 1992).

Thereby, $\mathcal{O}\big(\Sigma^{(4)}\big)$ denotes the partial derivative of the nonlinear observability map $q^{(4)}$ as defined on the right-hand side of (3.29)*. Hence, using the results of Example 3.2, local fault-detectability of the nonlinear problem has been verified.*

Similarly, local fault-isolability can be checked by verifying local observability of the augmented expressions $\Sigma^{(1,4)}$, $\Sigma^{(2,4)}$, and $\Sigma^{(3,4)}$. Performing the local observability analysis gives

$$\text{rank}\Big\{\mathcal{O}\big(\Sigma^{(1,4)}\big)\Big\} = 4,\ \forall\, u(t) \neq \text{const.},\ \forall\, x_P^{(1,4)} \in \mathbb{R}^{n_x^{(1,4)}} \tag{3.30}$$

for the first expression and

$$\text{rank}\Big\{\mathcal{O}\big(\Sigma^{(2,4)}\big)\Big\} = 4, \text{rank}\Big\{\mathcal{O}\big(\Sigma^{(3,4)}\big)\Big\} = 4,\ \forall\, u(t),\ \forall\, x_P^{(2,4),(3,4)} \in \mathbb{R}^{n_x^{(2,4),(3,4)}} \tag{3.31}$$

for $\Sigma^{(2,4)}$ and $\Sigma^{(3,4)}$ respectively. This result is quite interesting since it states (in combination with the results of Example 3.2) that the considered FDI problem is fault-isolable, if the DC drive is excited by the control input $u(t)$. Therefore, this problem configuration representatively exemplifies a practical class of systems which demand some excitation during the FDI process in order to remain fault-isolable.

3.4 FDI with Structured Augmented State Models

After investigating the modeling and analysis of systems being subject to faults, the attention is now turned towards the synthesis of FDI functions. In order to come up not only with persistent but also with intermittent faults, switching between the operating modes during the diagnosis process has to be considered by the underlying model and by the diagnosis method. Whereas in the FDI literature, various approaches address the non-switching diagnosis problem concerning persistent faults only (see e.g. (Tyler *et al.*, 2000; Rupp *et al.*, 2005; Ducard and Geering, 2006)), there are rather few methods coping with the more difficult problem of the switching case.

The idea to approach the general switching case is to employ hybrid (augmented) state estimation. Therefore, in the first instance, the fault diagnosis problem is specified as an optimal hybrid augmented state estimation problem. From this perspective, the optimal solution to fault diagnosis is then outlined basically relying on (Hofbaur, 2005). Thereby, it is not aimed at giving a complete review of hybrid state estimation. Rather, the intention is to highlight the parallels between nominal FDI and established hybrid state estimation methods. For an extensive discussion with respect to optimal hybrid estimation and the available sub-optimal methods of resolution, the interested reader is referred to the above referenced literature.

Given a sufficiently long input-/output-sequence (I/O-sequence) $\{u_\rho, y_\rho\}_0^k$ of system (3.1) and its corresponding structured augmented state model (3.17), the system can be diagnosed by determining an estimate $\hat{\chi}_k$ of the hybrid state

$$\chi_k = \big\langle (z_k = m_i), x_k^{(i)} \big\rangle. \tag{3.32}$$

This is a tuple $\langle\cdot\rangle$ of the discrete and the continuous state variables z_k and $x_k^{(\cdot)}$ respectively which contain the complete information for fault-detection, -isolation, and -identification (determining the fault-magnitude). Because the model (3.17) allows switching among the operating modes m_i, an adequate hybrid state estimator has to track possible trajectories $\mathcal{X}_k = \{\chi_\rho\}_0^k$ involving mode changes and determine their estimates $\hat{\mathcal{X}}_k = \{\hat{\chi}_\rho\}_0^k$. Obviously it lends itself to diagnose (3.1) by taking the whole sequence of available measurements $\{u_\rho, y_\rho\}_0^k$ into account. This helps to prevent false diagnosis, since in practical applications, measurements are always corrupted by noise. With this background information in mind, the considered FDI problem can be stated as follows.

Problem 3.1 (FDI of nominal and Gaussian noisy systems) *Let $\{u_\rho, y_\rho\}_0^k$ be a given I/O-sequence of the system $\Sigma(m_i)$. Then, using the structured augmented state model* (3.17)*, the fault diagnosis problem consists of determining the optimal hybrid state trajectory*

$$\hat{\mathcal{X}}_k^{\{\zeta\}} : \zeta = \underset{\beta=\{1,\ldots,\gamma_k\}}{\arg\max} \Psi_k^{\{\beta\}}, \tag{3.33}$$

where γ_k denotes the total number of possible trajectories (trajectory hypotheses) and $\Psi_k^{\{\beta\}} = \mathcal{C}\big(\hat{\mathcal{X}}_k^{\{\beta\}}, \{u_\rho, y_\rho\}_0^k\big)$ defines the path cost along the trajectory $\hat{\mathcal{X}}_k^{\{\beta\}}$ that quantifies the level of agreement between $\hat{\mathcal{X}}_k^{\{\beta\}}$ and $\{u_\rho, y_\rho\}_0^k$.

Remark 3.8 *Since a set of trajectory hypotheses is dealt with, a superscript index in curly brackets is used. For example $\hat{\mathcal{X}}_k^{\{\beta\}}$ refers to the β-th trajectory hypothesis $\hat{\mathcal{X}}_k^{\{\beta\}} = \big\{\ldots, \hat{\chi}_{k-1}^{\{\alpha\}}, \hat{\chi}_k^{\{\beta\}}\big\}$ which estimates a possible trajectory up to time k. This trajectory hypothesis includes the hybrid estimate $\hat{\chi}_k^{\{\beta\}}$ at its fringe. Note that the superscript index in curly brackets always refers to a trajectory hypothesis, whereas the superscript index in parentheses always refers to an operating mode.*

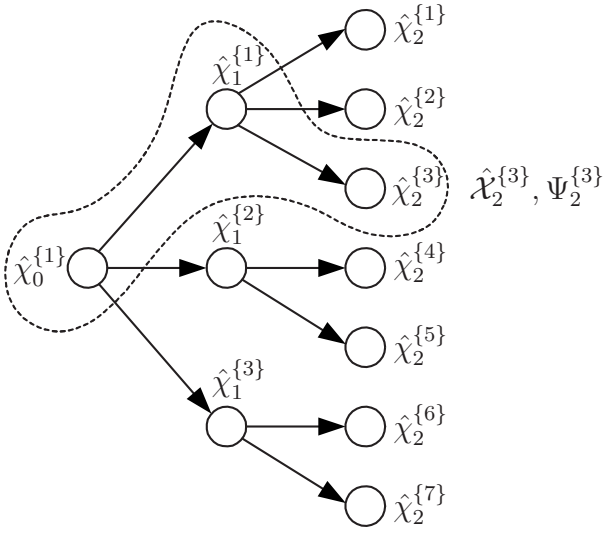


Figure 3.4: Exemplary full-hypothesis tree and trajectory path for behavior $\hat{\mathcal{X}}_2^{\{3\}}$ with cost $\Psi_2^{\{3\}}$ for the discrete-state automaton exemplified in Figure 3.2 ($\hat{z}_0^{\{1\}} = m_0$).

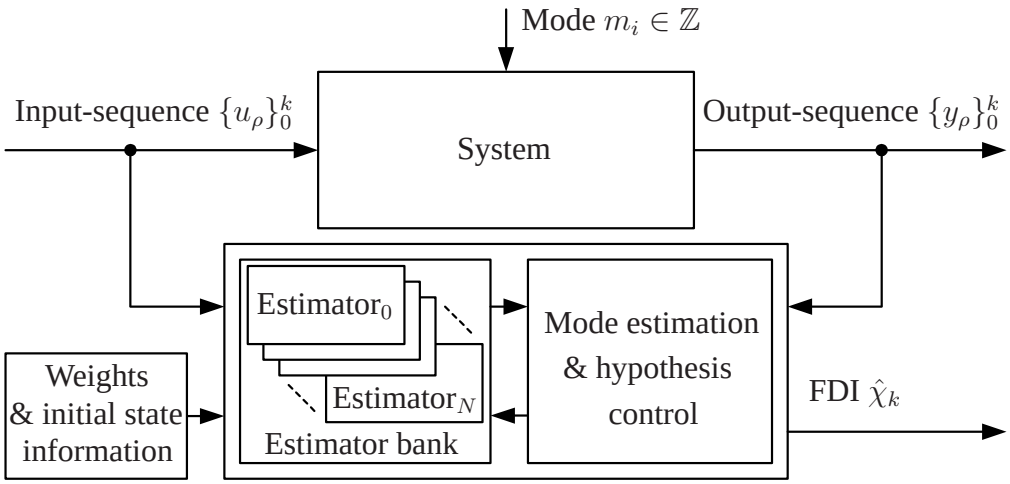


Figure 3.5: Full hypothesis hybrid estimation (fault diagnosis) architecture.

The optimal solution to the above stated fault diagnosis problem requires to build a full-hypothesis tree which encodes the estimates of all possible trajectories of (3.17) (see Figure 3.4). Therefore, any hypothesis $\hat{\mathcal{X}}_{k-1}^{\{\alpha\}}$ is extended with respect to the topology (given by the transition relation $\mathcal{G}$) of the automaton $\mathcal{A}$ by possible successor states $\hat{\chi}_k^{\{\beta\}}$ and new trajectory hypotheses $\hat{\mathcal{X}}_k^{\{\beta\}} = \left\{ \ldots, \hat{\chi}_{k-1}^{\{\alpha\}}, \hat{\chi}_k^{\{\beta\}} \right\}$ are obtained. It is worth to note that the optimization problem (3.33) uses an inverse formulation of the path cost aiming to maximize $\Psi_k^{\{\beta\}}$; which is in analogy to the probabilistic interpretation of the based hybrid estimation approach. Accordingly, the resulting γ_k hypotheses are ranked by their increasing path costs $\Psi_k^{\{\beta\}}$.

The employed trajectory-based estimation scheme uses the hybrid estimation architecture shown in Figure 3.5. The full hypothesis hybrid estimator consists of two components: An estimator bank that maintains one estimator per trajectory hypothesis, and a mode estimator that calculates the ranking among the hypotheses and initiates new estimators according to the trajectory hypotheses under consideration. Hence, the mode estimator controls the estimator bank that contains a monotonically growing number of dynamic estimators.

The number of involved trajectory hypotheses γ_k is exponential in the number of considered time steps k. Hence, rendering an optimal solution of the fault diagnosis problem is most often computationally intractable (Hofbaur, 2005). Therefore, the use of sub-optimal estimation approaches is indispensable for practical applications. In the literature, this problem has been addressed by a variety of authors, e.g. by (Ackerson and Fu, 1970; Blom and Bar-Shalom, 1988; Hofbaur and Williams, 2004). In order to gain a better understanding, this practicability issue is ignored for the moment. Instead a review on the optimal full hypothesis hybrid estimator is presented first. A practical sub-optimal approach to hybrid estimation is outlined in Section 3.5 and is illustrated by means of our running example of the DC actuator system.

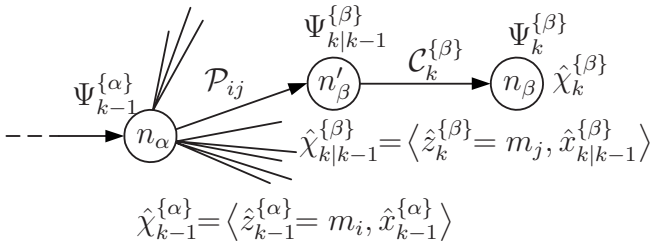


Figure 3.6: Two-step recursion in optimal hybrid estimation.

The fringe estimates $\hat{\chi}_k^{\{\beta\}}$ and their associated costs $\Psi_k^{\{\beta\}}$ are calculated according to the following two step process (see Figure 3.6):

• The *first step* determines possible mode transitions $\hat{z}_{k-1}^{\{\alpha\}} = m_i \rightarrow \hat{z}_k^{\{\beta\}} = m_j$, $(i,j) \in \{0,\ldots,N\}$, and predicts γ_k trajectory hypotheses

$$\hat{\mathcal{X}}_{k|k-1}^{\{\beta\}} = \Big\{ \ldots, \hat{\chi}_{k-1}^{\{\alpha\}} = \langle \hat{z}_{k-1}^{\{\alpha\}} = m_i, \hat{x}_{k-1}^{\{\alpha\}} = \hat{x}_{k-1}^{(i)} \rangle,\ \hat{\chi}_{k|k-1}^{\{\beta\}} = \langle \hat{z}_k^{\{\beta\}} = m_j, \hat{x}_{k|k-1}^{\{\beta\}} = \hat{x}_{k|k-1}^{(j)} \rangle \Big\}. \quad (3.34)$$

Thereby, the β-th prior fringe estimate $\hat{\chi}_{k|k-1}^{\{\beta\}}$ is a tuple of the mode estimate $\hat{z}_k^{\{\beta\}} = m_j$ and the augmented state $\hat{x}_{k|k-1}^{\{\beta\}}$ of the mode-conditioned continuous state prediction $\hat{x}_{k-1}^{\{\alpha\}} \rightarrow \hat{x}_{k|k-1}^{\{\beta\}}$.

• The *second step* takes the current measurement $\{u_k, y_k\}$ into account. It performs the correction of the predicted continuous state estimate $\hat{x}_{k|k-1}^{\{\beta\}} \rightarrow \hat{x}_k^{\{\beta\}}$. The cost of the corrected trajectory hypothesis $\hat{\mathcal{X}}_k^{\{\beta\}} = \big\{ \ldots, \hat{\chi}_k^{\{\beta\}} = \langle \hat{z}_k^{\{\beta\}}, \hat{x}_k^{\{\beta\}} \rangle \big\}$ is calculated recursively as

$$\Psi_k^{\{\beta\}} := \Psi_{k|k-1}^{\{\beta\}} + \mathcal{C}_k^{\{\beta\}}. \quad (3.35)$$

The predicted cost

$$\Psi_{k|k-1}^{\{\beta\}} = \Psi_{k-1}^{\{\alpha\}} + \mathcal{P}_{ij} \quad (3.36)$$

includes the weight $\mathcal{P}_{ij}$ of the corresponding mode transition $m_i \rightarrow m_j$. The hybrid observation function $\mathcal{C}_k^{\{\beta\}}$ is a cost term which quantifies the level of agreement between the prior hybrid state estimate $\hat{\chi}_{k|k-1}^{\{\beta\}}$ and the current measurement $\{u_k, y_k\}$.

Because the number of trajectory hypotheses grows with any time-step exponentially (see Figure 3.4), there is no computationally tractable approach to determine the outlined solution of the above stated fault diagnosis problem. However, the presented framework not only gives an exact system-theoretical specification of the FDI problem/task but also a comparison for practicable sub-optimal approaches. Furthermore it is pointed out that any sub-optimal estimation algorithm resulting in a sufficiently accurate approximation to the solution of the optimal hybrid estimation problem, provides also an adequate method for FDI. An excellent overview of various sub-optimal hybrid estimation schemes is contained in (Hofbaur, 2005). In (Aßfalg and Allgöwer, 2006*a*), a computationally tractable multiple-model approach to FDI is investigated employing the interacting multiple model algorithm (IMM). In (Aßfalg and Allgöwer, 2006*b*) FDI is performed by utilizing a K-step sub-optimal search method for hybrid estimation.

3.5 Example – Sub-Optimal FDI of the DC Actuator System

This chapter is concluded by another example investigating the sub-optimal FDI of the DC actuator (2.10) of Section 2.3. Again, it is restricted to the nominal case with $w_{1,k} = w_{2,k} = v_{1,k} = v_{2,k} = 0$.

3.5.1 Fault Representation and Fault Scenario

The DC actuator system is considered subject to the four fault-candidates $\mathcal{F}_1, \ldots, \mathcal{F}_4$, where abrupt and intermittent faults are assumed. Accordingly, each of the anticipated faults is represented by a constant-type exosystem

$$\Delta^{(i)} : \begin{cases} \xi^{(i)}_{k+1} = \xi^{(i)}_k,\ \xi^{(i)}_0,\ k \geq 0 \\ \xi^{(i)}_{\mathcal{H}} = 0 \\ \delta^{(i)}_k = \xi^{(i)}_k \\ \delta^{(i)}_{\mathcal{H}} = 0 \end{cases} , \ i \in \{1, \ldots, 4\}\,. \tag{3.37}$$

The resulting set of modes $\mathbb{Z} = \{m_0, m_1, \ldots, m_4\}$ is given by the fault-free mode m_0 and by the modes $m_1, \ldots, m_4$ being due to the anticipated faults $\mathcal{F}_1, \ldots, \mathcal{F}_4$. Assuming a classical single-fault scenario, possible mode transitions $\mathbb{Z} \to \mathbb{Z}$ are ruled by a discrete-state automaton $\mathcal{A}$ which describes the mode transition relation of Figure 3.7. According to the hybrid estimation approach of Section 3.4, each mode transition $m_j \to m_i$ is weighted by the scalar cost term $\mathcal{P}_{ij}$. By assigning a zero-weight to each of the nonexistent mode transitions (e.g. $P_{14} = 0$, see Figure 3.7), the discrete-state automaton $\mathcal{A}$ can be completely described by the mode-set $\mathbb{Z}$ and by the (square) $N+1$-dimensional adjacency matrix

$$\mathcal{P} = \begin{bmatrix} \mathcal{P}_{00} & \mathcal{P}_{01} & \ldots & \mathcal{P}_{04} \\ \mathcal{P}_{10} & \mathcal{P}_{11} & \ldots & \mathcal{P}_{14} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{P}_{40} & \mathcal{P}_{41} & \ldots & \mathcal{P}_{44} \end{bmatrix} , \text{ with } \sum_{i=0}^{N=4} \mathcal{P}_{ij} = 1,\ \forall\, j = 0, \ldots, 4. \tag{3.38}$$

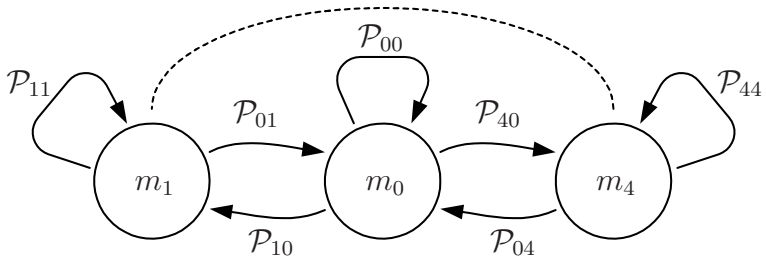


Figure 3.7: Mode transition graph of the state automaton $\mathcal{A}$ describing the based single-fault scenario.

In case of the exemplified DC actuator system, the 4×4-dimensional adjacency matrix is chosen as follows:

$$\mathcal{P} = \begin{bmatrix} 0.90 & 0.15 & 0.15 & 0.15 \\ 0.1/3 & 0.85 & 0.00 & 0.00 \\ 0.1/3 & 0.00 & 0.85 & 0.00 \\ 0.1/3 & 0.00 & 0.00 & 0.85 \end{bmatrix}.$$

The matrix $\mathcal{P}$ is a stochastic weighting matrix with column entries adding to one. Thereby, mode transitions that occur with high probability are weighted higher, close to one. On the other hand, unlikely mode transitions are weighted lower, close to zero. Because the fault-free mode m_0 is also a special case of the fault modes m_i, $i \in \{1, \ldots, N\}$ (which effectuates some non-uniqueness of the fault-free case, see Section 3.3), it is required to be treated separately. To that effect, the highest weights (e.g. $\mathcal{P}_{00} = 0.9$, $\mathcal{P}_{10} = 0.85$) are assigned to the transitions being directed at the fault-free mode m_0. The most likely operation of the system is usually the fault-free mode which is why the highest weight $\mathcal{P}_{00} = 0.9$ is assigned to its self-transition. It remains to be seen that this certain choice of weights causes the FDI function to tend to the fault-free mode whenever there is no fault clearly indicated by the measurements.

3.5.2 Structured Augmented State Model of the DC Actuator System

The structured augmented state model of the exemplified DC actuator system is given by the tuple

$$\mathcal{S} := \Big\{ \{\Sigma^{(i)}, i \in \{0, \ldots, 4\}\}, \mathcal{A}(\mathbb{Z}, \mathcal{P}) \Big\}, x_0^{(i)}, z_0 = m_0. \tag{3.39}$$

This includes the discrete-state automaton $\mathcal{A}$ in terms of the mode-set $\mathbb{Z}$ and the adjacency matrix $\mathcal{P}$ as well as the mode-conditioned augmented state models $\Sigma^{(i)}$, $i \in \{0, \ldots, 4\}$. Each of the augmented state models is determined as a concatenation $\Sigma^{(i)} = \Sigma \circ \Delta^{(i)}$ that extends the nominal actuator model (2.10) by the corresponding mode-specific exosystem (3.37), i.e.,

$$\Sigma^{(0)} \quad : \quad \begin{cases} u'_k = u_k \\ x^{(0)}_{1,k+1} = x^{(0)}_{1,k} + \dfrac{dT}{L}\big(- R\, x^{(0)}_{1,k} - k_m\, x^{(0)}_{2,k} + u'_k \big) \\ x^{(0)}_{2,k+1} = x^{(0)}_{2,k} + \dfrac{dT}{J}\big(k_m\, x^{(0)}_{1,k} - d\, x^{(0)}_{2,k} \big) \\ y_{1,k} = x^{(0)}_{1,k} \\ y_{2,k} = x^{(0)}_{2,k} \end{cases}, x_0^{(0)} = \begin{bmatrix} x^{(0)}_{1,0} \\ x^{(0)}_{2,0} \end{bmatrix}$$

$$\Sigma^{(1)} \quad : \quad \begin{cases} u'_k = u_k + x^{(1)}_{3,k} \\ x^{(1)}_{1,k+1} = x^{(4)}_{1,k} + \dfrac{dT}{L}\big(- R\, x^{(1)}_{1,k} - k_m\, x^{(1)}_{2,k} + u'_k\big) \\ x^{(1)}_{2,k+1} = x^{(1)}_{2,k} + \dfrac{dT}{J}\big(k_m\, x^{(1)}_{1,k} - d\, x^{(1)}_{2,k}\big) \\ x^{(1)}_{3,k+1} = x^{(1)}_{3,k} \\ y_{1,k} = x^{(1)}_{1,k} \\ y_{2,k} = x^{(1)}_{2,k} \\ \vdots \end{cases} , x^{(1)}_0 = \begin{bmatrix} x^{(1)}_{1,0} \\ x^{(1)}_{2,0} \\ x^{(1)}_{3,0} \end{bmatrix}.$$

Thereby, mismatched fault characteristics are set to their fault-free values, i.e., $\delta^{(j)}_k := \delta^{(j)}_{\mathcal{H}} = 0$, $j \neq i \in [0, \ldots, 4]$, and $x^{(0)}_k = [x_{1,k}\ x_{2,k}]^T$, $x^{(1)}_k = [x_{1,k}\ x_{2,k}\ \xi^{(1)}_k]^T$.

3.5.3 FDI by Using Sub-Optimal IMM-EKF Hybrid Estimation

In order to solve Problem 3.1 for the exemplified DC actuator system, the well-known sub-optimal interacting multiple model algorithm (IMM) is employed in combination with an extended Kalman filter (EKF). In the following, only the application of this commonly used combination is investigated. For more detailed considerations with respect to these algorithms and their background, the interested reader is referred to the literature (Blom and Bar-Shalom, 1988; Li and Bar-Shalom, 1996; Hofbaur, 2005) and (Gelb *et al.*, 1974; Boutayeb *et al.*, 1997) respectively.

3.5.3.1 Sub-Optimal IMM-EKF Hybrid Augmented State Estimation

A good trade-off between computational cost and hybrid estimation quality is achieved by the IMM algorithm. The IMM reduces the exponentially growing number of hypotheses γ_k to the fixed number of modes $N + 1$ by merging trajectory hypotheses which share the same mode at their fringe. In this way, the IMM achieves a good trade-off between computational cost and estimation quality (Blom and Bar-Shalom, 1988). Using the IMM for the solution of Problem 3.1, the predicted cost (3.36) is computed as

$$\Psi^{(j)}_{k|k-1} = \sum_{i=0}^{N} \mathcal{P}_{ij} \Psi^{(i)}_{k-1}, \tag{3.40}$$

where the free parameters $\mathcal{P}_{ij}$ weight the transitions between the modes m_i and m_j. On the basis of the actual measurements $\{u_k, y_k\}$, the IMM approximates the corrected cost (3.35) as

$$\Psi^{(j)}_k = \mathcal{C}^{(j)}_k\, \Psi^{(j)}_{k|k-1} \left(\sum_{i=0}^{N} \mathcal{C}^{(i)}_k\, \Psi^{(i)}_{k|k-1} \right)^{-1}. \tag{3.41}$$

In (3.41), the hybrid observation function $\mathcal{C}_k^{(j)}$ describes a cost term that quantifies the level of agreement between the measurements $\{u_k, y_k\}$ and the model being conditioned on the mode m_j. The hybrid observation function is computed as

$$\mathcal{C}_k^{(j)} = \frac{1}{|2\pi\Lambda_k^{(j)}|^{1/2}} \exp\Big(-0.5 \,\big|\big|\Delta y_k^{(j)}\big|\big|^2_{\Lambda_k^{(j)-1}}\Big). \tag{3.42}$$

The residual $\Delta y_k^{(j)}$ and the associated (covariance) matrix $\Lambda_k^{(j)}$ result from the innovation step of the involved mode-conditioned EKF continuous-state estimation which is performed recursively at any time k. In turn, the state and covariance extrapolation step of the EKF is based on the following mixed expressions:

$$\begin{aligned} \bar{x}_{k-1}^{(j)} &= \sum_{i=0}^{N} \hat{x}_{k-1}^{(i)}\, \mu_{ij} \\ \bar{P}_{k-1}^{(j)} &= \sum_{i=0}^{N} \Big(P_{k-1}^{(i)} - (x_{k-1}^{(i)} - \bar{x}_{k-1}^{(j)})(x_{k-1}^{(i)} - \bar{x}_{k-1}^{(j)})^T \Big)\, \mu_{ij}; \end{aligned} \tag{3.43}$$

where the $(N+1)^2$ mixing-weights μ_{ij} specify the level of interaction among the operation modes m_i. These are determined as

$$\mu_{ij} = \mathcal{P}_{ij}\, \Psi_{k-1}^{(i)} (\Psi_{k|k-1}^{(j)})^{-1}. \tag{3.44}$$

The one-step ahead prediction of the involved mode-conditioned EKF employs the mixed expressions (3.43) for re-initialization as

$$\hat{x}_{k|k-1}^{(j)} = f^{(j)}\big(\bar{x}_{k-1}^{(j)}, u_{k-1}\big),\ P_{k|k-1}^{(j)} = A_k^{(j)} \bar{P}_{k-1}^{(j)} A_k^{(j)T} + Q_k^{(j)} \tag{3.45}$$

and determines the prediction residual $\Delta y_k^{(j)}$ and the associated covariance matrix $\Lambda_k^{(j)}$ with

$$\Delta y_k^{(j)} = y_k - h^{(j)}\big(\hat{x}_{k|k-1}^{(j)}, u_k\big),\ \Lambda_k^{(j)} = C_k^{(j)} P_{k|k-1}^{(j)} C_k^{(j)T} + R_k^{(j)}. \tag{3.46}$$

This is followed by the estimation correction step for the computation of the mode-conditioned continuous augmented state $\hat{x}_k^{(j)}$ and the associated (covariance) matrix $P_k^{(j)}$ as

$$\hat{x}_k^{(j)} = \hat{x}_{k|k-1}^{(j)} + K_k^{(j)} \Delta y_k^{(j)},\ P_k^{(j)} = P_{k|k-1}^{(j)} - K_k^{(j)} \Lambda_k^{(j)} K_k^{(j)T}. \tag{3.47}$$

Both $\hat{x}_k^{(j)}$ and $P_k^{(j)}$ form the basis for (3.43) in the next IMM step. Thereby, the Kalman gain $K_k^{(j)}$ is computed by

$$K_k^{(j)} = P_{k|k-1}^{(j)} C_k^{(j)T} \Lambda_k^{(j)-1} \tag{3.48}$$

and

$$A_k^{(j)} = \left.\frac{\partial f^{(j)}}{\partial x^{(j)}}\right|_{\hat{x}_{k-1}^{(j)}, u_{k-1}},\ C_k^{(j)} = \left.\frac{\partial h^{(j)}}{\partial x^{(j)}}\right|_{\hat{x}_{k|k-1}^{(j)}, u_k}. \tag{3.49}$$

The IMM-EKF algorithm necessitates the following initialization variables to be set: The $N+1$ initial continuous-states $\hat{x}_0^{(j)}$, the initial (covariance) matrices $P_0^{(j)} \geq 0$, and the initial costs $\Psi_0^{(j)}$. Furthermore, the IMM has to be parameterized by the $N+1$-dimensional weighting matrix $\mathcal{P}$ (with elements satisfying $\sum_{i=0}^{N} \mathcal{P}_{ij} = 1,\ \forall\, j = 0, \ldots, N$). The EKF has to be tuned by setting the $N+1$ matrices $Q_k^{(j)} \geq 0$ and $R_k^{(j)} \geq 0$.

Remark 3.9 *Whenever the approximation of the nonlinear system in terms of the first-order Taylor-series expansion* (3.49) *is insufficient, one could use higher-order Taylor series expansions that lead to higher-order EKFs (Gelb* et al.*, 1974), apply the unscented Kalman filter (Julier and Uhlmann, 1997), or use other estimation techniques that were developed for the state estimation of nonlinear systems.*

Finally, the IMM-EKF hybrid estimator is summarized in the following recursive algorithm.

Algorithm 3.1 (IMM-EKF hybrid estimation) *Suppose the structured augmented state model $\mathcal{S}$ and the sufficiently long I/O-sequence $\{u_\rho, y_\rho\}_0^k$ to be given. Determine the IMM-EKF hybrid estimation algorithm*

$$\text{IMM-EKF}\Big(\mathcal{S}, \big\{u_\rho, y_\rho\big\}_0^k\Big) = \Big\{\hat{x}_k^{(j)}, \Psi_k^{(j)}\Big\}. \tag{3.50}$$

The operator IMM-EKF$(\cdot)$ comprises the following computation steps that are executed recursively over the sequence $\rho \in \{0, \ldots, k\}$:

1. *Compute the predicted cost* (3.40)*, determine the mixing-weights* (3.44)*, and evaluate the mixed state and covariance expressions* (3.43)*.*

2. *Perform the one-step ahead prediction of the continuous-state according to* (3.45) *and determine the hybrid observation function* (3.42) *by using* (3.46)*.*

3. *Compute the corrected cost* (3.41)*, correct the continuous-state estimate according to* (3.47)*, and enter the next recursion with the first step.*

3.5.3.2 Fault Diagnosis by Using the Sub-Optimal IMM-EKF Algorithm

It is clear from the previous considerations that the fault diagnosis of the DC actuator system can be computed as follows:

$$\hat{\chi}_k = \big\langle (\hat{z}_k = m_\zeta), \hat{x}_k^{(\zeta)} \big\rangle : \zeta = \underset{j \in \{0,\ldots,N\}}{\arg\max}\ \Psi_k^{(j)}; \tag{3.51}$$

where $\hat{x}_k^{(j)}$ and $\Psi_k^{(j)}$ are calculated recursively by using Algorithm 3.1. Hence, the fault diagnosis $\hat{\chi}_k$ is determined by the tuple $\big\langle (\hat{z}_k = m_\zeta), \hat{x}_k^{(\zeta)} \big\rangle$ that maximizes the corrected (inverse) path cost $\Psi_k^{(j)}$.

3.5.4 Numerical Results

The numerical simulation is performed by using a MATLAB/SIMULINK implementation of Algorithm 3.1. The FDI of the DC actuator system is computed under the terms of (3.51). According to the results of the fault-detectability and -isolability analysis of Example 3.3, the DC drive is persistently excited by a sinusoidal control input u_k in order to ensure local fault-isolability during the FDI process. Table 3.1 summarizes the imposed fault scenario and the fault magnitudes which impact the system subsequently. In Figure 3.8 the results obtained from the sub-optimal IMM-EKF hybrid estimation scheme are shown. Thereby, the faults $\mathcal{F}_1, \ldots, \mathcal{F}_4$ occurred intermittently under the terms of the test sequence summarized in Table 3.1.

Table 3.1: Overview of the example fault-scenario with $t_{\mathcal{F}}$ and $t_{\mathcal{H}}$ denoting the specific time of fault-occurrence and -recovery respectively.

Fault	Description	Maximum fault-magnitude	Unit	$t_{\mathcal{F}}$, $t_{\mathcal{H}}$ [s]
$\mathcal{F}_1$	Input-fault (fault in power supply)	$\delta^{(1)}_{\max} = 0.6$	[V]	$5, 20$
$\mathcal{F}_2$	Output-fault (fault in current sensor)	$\delta^{(2)}_{\max} = 0.15$	[A]	$25, 40$
$\mathcal{F}_3$	Output-fault (fault in angular sensor)	$\delta^{(3)}_{\max} = 6.0$	[rad/s]	$45, 60$
$\mathcal{F}_4$	System-fault (fault in Ohmic resistor)	$\delta^{(4)}_{\max} = 0.6$	[Ω]	$65, 80$

Figure 3.8 a) demonstrates that the faults $\mathcal{F}_1, \ldots, \mathcal{F}_4$ are detected, isolated, and identified beyond the limitations imposed by the unstructured augmented state observability. Furthermore, all of the operating modes are estimated without significant time-delays. In Figure 3.8 b), the estimated

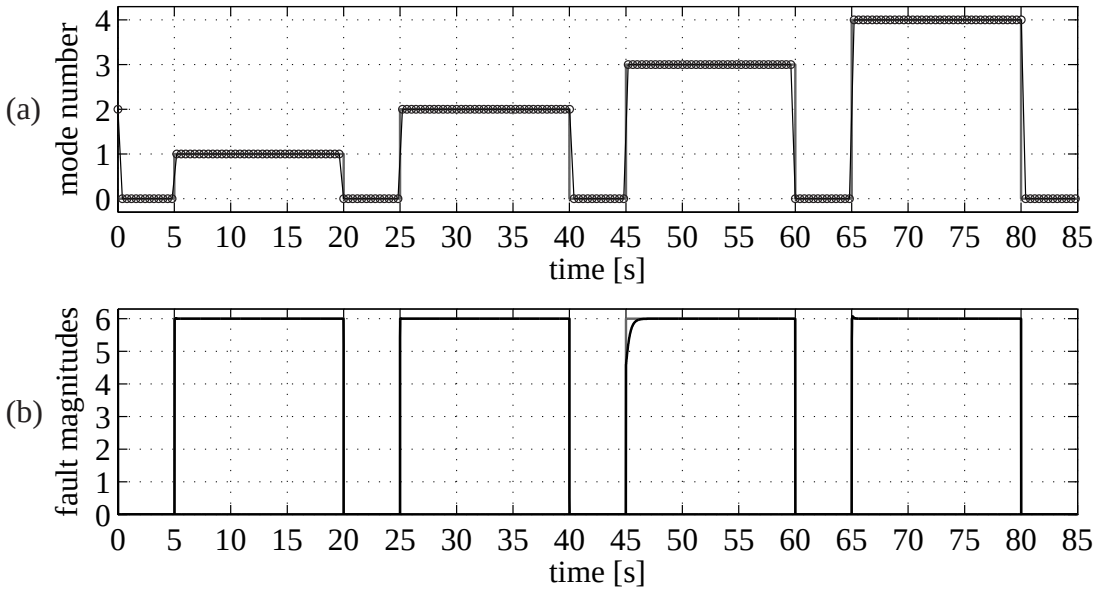


Figure 3.8: Sub-optimal FDI of the DC actuator system. (a) Imposed (gray solid) and estimated (black circled) mode sequences. (b) Imposed (gray) and estimated (black) normalized fault magnitudes.

fault-magnitudes $\delta_k^{(1)}, \ldots, \delta_k^{(4)}$ are shown to determine a sufficiently accurate fault-identification. By this means, the internal model formulation gives also estimates of the real values $y'_k = [x_{1,k}\, x_{2,k}]^T$, despite of the output-faults $\mathcal{F}_2$ and $\mathcal{F}_3$. This additional feature could be also very useful for fault-tolerant control if the controller is fed by the estimated output $\hat{y}'_k$.

As becomes clear from this example, the setup and solution algorithm do indeed lead to a superb FDI performance despite the rather general problem setup.

3.6 Summary

The augmented state modeling approach is demonstrated to be particularly practicable for representing systems which operate subject to potential faults. It proves to be very attractive since both model-based FDI and diagnosability analysis can be performed by utilizing established methods from the field of state estimation and observability analysis respectively. Thus, even for the challenging tasks of nonlinear FDI and diagnosability analysis, practicable methods are available. However, this approach entails a severe drawback: In real FDI problems, potential faults rarely affect a system all at the same time. Therefore the unstructured augmented state modeling approach is conservative and it is restricted by the unstructured augmented state observability to problems with a limited number of faults.

In order to overcome these limitations, the formalism of structured augmented state models has been introduced. Similar to the most commonly encountered FDI approaches, faults are assumed to occur under the terms of a predefined fault scenario. By incorporating these additional constraints into the model in form of a discrete-state automaton, the FDI problem is transformed from a continuous augmented state estimation problem to a hybrid augmented state estimation problem. Accordingly, fault-detectability and -isolability analysis can be approached as special cases of hybrid state observability analysis. By exploiting the relationships between FDI and hybrid estimation, practicable methods for fault-detectability and -isolability analysis are provided. These methods extend the approaches found in the FDI literature and furthermore, prove the gain of observability as originally intended by introducing the structured augmented state modeling formalism. From a hybrid estimation perspective, the nominal FDI problem is specified and its optimal solution is discussed. Since this considers the general (switching) case, intermittent as well as persistent faults can be diagnosed, which is again an improvement of published FDI approaches.

Based on the DC actuator example, the fault-detectability and -isolability analysis for different linear and nonlinear problem configurations is illustrated. Particularly for linear systems, the provided analysis methods prove to be very applicable even to complex high-dimensional systems operating subject to a large number of fault candidates. In the nonlinear case, the suggested analysis methods encounter the same limitations as the related methods of nonlinear observability analy-

sis. Hence, their application is usually limited to the analysis of rather simple, low-dimensional nonlinear systems.

By utilizing the sub-optimal IMM-EKF hybrid estimation scheme, the FDI of the nonlinear DC actuator has been demonstrated. Beyond the observability limitations of the unstructured approach, all faults are detected, isolated, and identified correctly without significant time-delay. From a methodic point of view, it is particularly remarkable that the nonlinear FDI of the DC actuator system can be performed in a straightforward application of the sub-optimal IMM-EKF approach to hybrid estimation. Because no specific properties of the diagnosed system have to be considered, the suggested approach is very general and proves to be applicable to a wide class of practical problems appearing in the field of FDI.

Chapter 4

Robust FDI with Uncertain Structured Augmented State Models

In this chapter, the robust FDI of nonlinear systems is treated. The nominal structured augmented state model is extended to the uncertain case including continuous modeling uncertainties as well as unanticipated faults. After reviewing the background of nonlinear set-valued augmented state estimation, the synthesis of robust FDI algorithms is investigated. A novel and computationally tractable on- and off-line FDI architecture is provided that, under certain conditions, is guaranteed to determine a robust FDI of persistent and intermittent fault-types and furthermore is capable to cope with unanticipated faults. Robust fault-detection and -isolation conditions are derived by which a meaningful and non-trivial result is obtained by the suggested FDI algorithm. The results are illustrated by means of the DC actuator example.

One of the most important conditions precedent to practicability of model-based FDI functionalities is the robustness against uncertainties of the underlying model. In FDI, modeling uncertainties not only include plant-model-mismatch but also unavoidable errors in the anticipated faults' representation as well as unanticipated faults.

In recent years, there has been considerable research activity aimed at the design of robust FDI schemes specific for nonlinear systems. In (Frank, 1994), (Hammouri *et al.*, 1999), and (C. De Persis and A. Isidori, 1999) the FDI problem has been addressed in the case of nonlinear systems in which the structured uncertainties of the system model and the faults can be decoupled. Besides these promising approaches, there have not been many analytical results on FDI in the case of unstructured modeling uncertainties that cannot be exactly decoupled from the potential faults. In (Zhang *et al.*, 2002) a neural-network-based approach to the robust FDI of structured/unstructured nonlinear systems is suggested which, however, is restricted to the rather small class of systems with full-state measurements.

Particularly robust FDI methods addressing continuous modeling uncertainties have attracted a lot of attention. However, there are not many approaches that can cope with discrete-type uncertainties like unanticipated faults causing a system to work in an unknown mode of operation. In (Farrell *et al.*, 1993) on-line learning techniques are suggested to accommodate this problem. Whereas the concept of the unknown mode is central to discrete model-based FDI (Hamscher, 1992; De Kleer and Williams, 1987; De Kleer and Williams, 1989), there are not many methods that address this difficult type of uncertainty problem in the continuous case.

This chapter contributes in three ways to the robust FDI of nonlinear systems: On the basis of a general class of nonlinear systems, our nominal structured augmented state model is extended to the uncertain case. This includes structured/unstructured uncertainties of the employed system and fault representation and furthermore includes unanticipated faults by means of an unknown mode of operation. Thereby, continuous uncertainties are described using the useful and easily applicable unknown-but-bounded uncertainty representation. The resulting uncertain structured augmented state model is summarized in Definition 4.1. Based on this model, a generally applicable robust FDI algorithm (Algorithm 4.3) is introduced, allowing to compute a robust FDI of anticipated/unanticipated persistent and intermittent fault-types in the presence of the above referred uncertainties (Theorem 4.2). Robust fault-detectability and -isolability conditions are derived (Theorem 4.3 and 4.4) by which the proposed FDI algorithm is guaranteed to determine a meaningful, i.e., a non-trivial result.

4.1 Uncertain Structured Augmented State Model

In Chapter 3, the hybrid modeling formalism of structured augmented state models was introduced in the nominal framework. This approach is now extended to the uncertain case as it has been originally introduced in Section 2.1. For this purpose, the model of Definition 3.1 is subsequently extended with respect to the following uncertainties:

1. The *uncertainty of the continuous (quantitative) part model* $\left\{\Sigma^{(i)}, i \in \{0,\ldots,N\}\right\}$ including the plant-model mismatch due to disturbances, modeling uncertainties and measurement noise (see Section 2.1). Furthermore, additional uncertainties which inevitably appear due to the choice of fault-specific exosystems (3.2) are considered.

2. The *uncertainty of the discrete (qualitative) part model* $\mathcal{A}(\cdot)$ which includes unknown operating modes that are due to unforeseen faults being unanticipated by the model and by the supposed fault-scenario.

In the following, the individual kinds of model uncertainties are briefly discussed and factored into the parts of the nominal model (3.17). The resulting setup is finally summarized by means

of the *uncertain structured augmented state model* which provides the basis for the subsequent investigations with respect to robust FDI.

4.1.1 Uncertainty of the Continuous Part Model

This chapter recalls and extends the uncertain system model (2.1) and (2.4) as originally introduced in Section 2.1. Again faults are represented by dynamical exosystems (3.2) which, however, are now considered to be uncertain.

In practical FDI applications, the time responses of the fault-specific signals $\delta_k^{(i)}$ are generally hard to predict and certainly the same holds for the dynamics of the corresponding exosystem models. Considering the (fictitious) exosystem $\Delta^{\star(i)}$ which is supposed to describe the fault $\mathcal{F}_i$ exactly, the mismatch between $\Delta^{\star(i)}$ and its approximation $\Delta^{(i)}$ chosen by the design engineer entails another uncertainty that has to be regarded during the robust FDI design process. By introducing the unknown-but-bounded uncertainty input

$$\lambda_k^{(i)} \in \mathbb{L}_k^{(i)} \subset \mathbb{R}^{n_\lambda^{(i)}} \tag{4.1}$$

for representing the mismatch between $\Delta^{\star(i)}$ and $\Delta^{(i)}$, the i-th uncertain exosystem-model takes the following form

$$\Delta^{(i)}: \begin{cases} \xi_{k+1}^{(i)} = \phi^{(i)}\big(\xi_k^{(i)}, \lambda_k^{(i)}\big),\ \xi_0^{(i)},\ k \geq 0 \\ \xi_{\mathcal{H}}^{(i)} = 0 \\ \delta_k^{(i)} = \psi^{(i)}\big(\xi_k^{(i)}, x_k, u_k\big) \\ \delta_{\mathcal{H}}^{(i)} = \text{const.} \end{cases} . \tag{4.2}$$

Remark 4.1 *Note that the uncertain exosystem model* (4.2) *refrains from introducing another unknown-but-bounded input characterizing the uncertainty of the exosystem's output equation. However, this is not restrictive since in the bottom-up system model Σ (system model (2.1)), such uncertainties are already captured by the inputs w_k and v_k.*

Again, merging of the models (2.1), (2.4), (4.1), and (4.2) leads to $N+1$ uncertain augmented state models

$$\Sigma^{(i)}: \begin{cases} x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}, u_k, w_k^{(i)}\big), x_0^{(i)},\ k \geq 0 \\ y_k = h^{(i)}\big(x_k^{(i)}, u_k, v_k^{(i)}\big) \end{cases}, \tag{4.3}$$

each characterizing an operating mode m_i. Thereby, the augmented uncertainty inputs $w_k^{(i)} \in \mathbb{R}^{n_w^{(i)}}$ and $v_k^{(i)} \in \mathbb{R}^{n_v^{(i)}}$ lump the unknown-but-bounded uncertainties w_k, v_k, and $\lambda_k^{(i)}$, whereas an analog aggregation of the sets $\mathbb{W}_k$, $\mathbb{V}_k$, and $\mathbb{L}_k^{(i)}$ leads to the compact bounding sets $\mathbb{W}_k^{(i)}$ and $\mathbb{V}_k^{(i)}$ respectively. Because the augmented initial state $x_0^{(i)}$ is unknown in most applications, it lends itself to introduce another set $\hat{\mathbb{X}}_0^{(i)}$ for uniformly bounding the initial state uncertainty of the augmented system (4.3). With respect to the uncertainties of system (4.3), the following assumption holds.

Assumption 4.1 *The initial augmented state $x_0^{(i)}$ and the augmented exogenous inputs $w_k^{(i)}$ and $v_k^{(i)}$ are each unknown-but-bounded by some compact set for all times, i.e., they all satisfy the following uncertainty model*

$$\Omega^{(i)} : \left\{ x_0^{(i)} \in \hat{\mathbb{X}}_0^{(i)} \subset \mathbb{R}^{n_x^{(i)}},\, w_k^{(i)} \in \mathbb{W}_k^{(i)} \subset \mathbb{R}^{w_x^{(i)}},\, v_k^{(i)} \in \mathbb{V}_k^{(i)} \subset \mathbb{R}^{n_v^{(i)}},\, \forall\, k. \right. \tag{4.4}$$

By means of the model (4.3) and the unknown-but-bounded uncertainty representation (4.4), any operating mode m_i, $i \in \{0, \ldots, N\}$ of the system (2.1) can be described as a tuple $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$. In the following subsection, each of these tuples is assigned to a specific operating mode of the discrete part model.

4.1.2 Uncertainty of the Discrete Part Model

Similar to standard multiple-models for FDI, the formalism of structured augmented state models assumes the system to operate in a mode of operation that is captured by the model (see Assumption 3.1). Nevertheless, unanticipated faults do occur in real world systems and existing robust FDI methods based on such idealized models either fail to isolate such unusual operational conditions or perform in an unexpected way. In the worst case, their robustness may even lead to false diagnosis. Hence, it is desirable to extend the employed modeling formalism so that a bottom-up FDI capability can cope with such an *unknown mode* of operation.

By introducing an additional candidate $\mathcal{F}_?$ for unanticipated single- or multiple-faults, the nominal set (2.3) can be reformulated as follows:

$$\mathbb{F}_? = \left\{ \mathcal{F}_1, \ldots, \mathcal{F}_N, \mathcal{F}_? \right\}. \tag{4.5}$$

According to the extended set of fault candidates (4.5), a reformulation of the nominal set of modes (3.12) has to be conducted giving

$$\mathbb{Z}_? = \left\{ m_0 : \left(\Sigma^{(0)}, \Omega^{(0)}\right), m_1 : \left(\Sigma^{(1)}, \Omega^{(1)}\right), \ldots, m_N : \left(\Sigma^{(N)}, \Omega^{(N)}\right), m_? : \left(\Sigma^{(?)}, \Omega^{(?)}\right) \right\}. \tag{4.6}$$

Thereby, the unknown mode $m_?$ is characterized by means of a fictitious uncertain model that is described by two empty sets of equations

$$\Sigma^{(?)} = \{\cdot\}, \Omega^{(?)} = \{\cdot\}. \tag{4.7}$$

In contrast to the nominal sets $\mathbb{F}$ and $\mathbb{Z}$ (see equations (3.11) and (3.12)), no critical assumption about the completeness of $\mathbb{F}_?$ and $\mathbb{Z}_?$ has to be met (see also Remark 2.1). Rather, the sets $\mathbb{F}_?$ and $\mathbb{Z}_?$ are inherently complete. This property is captured by the following lemma.

Lemma 4.1 *The extended set of potential fault candidates $\mathbb{F}_?$ and the extended set of modes $\mathbb{Z}_?$ are inherently complete. Therefore, any fault that potentially affects the system 2.1, i.e., any operating mode of the system has to come forward as a candidate of these sets.*

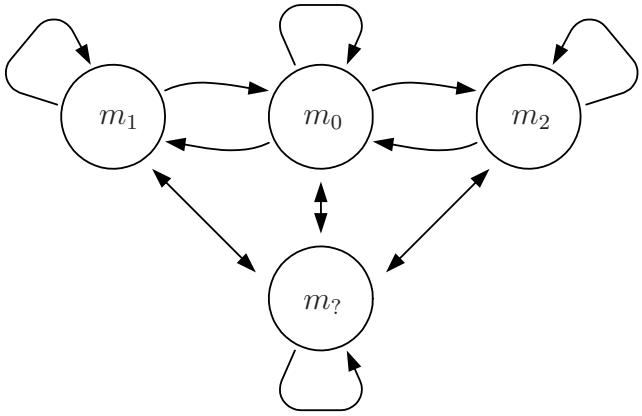


Figure 4.1: Exemplary mode transition graph of a system operating subject to two known single-fault candidates $\mathcal{F}_{1,2}$ and an unknown single- or multiple-fault candidate $\mathcal{F}_?$.

Proof. The proof of this lemma is trivial since it directly follows from the definition of the unanticipated fault candidate $\mathcal{F}_?$. Because this can be of both single- and multiple-fault type, all kinds of unanticipated fault situations are covered: Unanticipated single-faults, unanticipated multiple-faults, and anticipated faults occurring in unforeseen combinations that are unconsidered by the underlying fault scenario. ■

Remark 4.2 *Note that the unknown mode $m_?$ is used as a substitute that covers any system operation which remains unanticipated during the modeling process. A discrimination between different unanticipated faults being lumped in this mode, is not possible.*

The additional mode $m_?$ requires the topology of the discrete-state automaton $\mathcal{A}$ (see equation (3.16)) to be adapted so that the unknown-mode $m_?$ is reachable from any anticipated mode $m_0, \ldots, m_N$ and vice versa (see Figure 4.1). The resulting uncertain discrete-state automaton is described by means of the following tuple

$$\mathcal{A}_?\big(\mathbb{Z}_?, \mathcal{G}_? : \mathbb{Z}_? \rightarrow \mathbb{Z}_?\big),\ z_0. \tag{4.8}$$

This includes the mode set $\mathbb{Z}_?$, the uncertain discrete-state transition relation $\mathcal{G}_?$ comprising the unknown mode, and the initial discrete-state z_0.

4.1.3 Uncertain Structured Augmented State Model

Similar to the nominal case, the individual model fragments are combined in a tuple. The resulting hybrid-state automaton is summarized in the following definition and is further referred to as *uncertain structured augmented state model*.

Definition 4.1 (Uncertain structured augmented state model) *An uncertain structured augmented state model is described as a tuple*

$$\mathcal{S}_\mathcal{U} := \left(\left\{\left(\Sigma^{(i)}, \Omega^{(i)}\right), i \in \{0, \ldots, N\}, \left(\Sigma^{(?)}, \Omega^{(?)}\right)\right\}, \mathcal{A}_?\right),\ x_0^{(i)}, z_0. \tag{4.9}$$

This aggregates the $N+1$ mode-conditioned uncertain augmented state models ((4.3),(4.4)*), the empty sets of equations* (4.7)*, and the uncertain discrete-state automaton* (4.8)*.*

The uncertain and the nominal structured augmented state model are constructed in the same way and can be both illustrated by the block diagram shown in Figure 3.3. However, they use different expressions for the continuous part model of the system and the faults as well as for the associated discrete-state automaton.

4.2 Nonlinear Set-Valued Augmented State Estimation

As in the nominal case, augmented state estimation will also play a key role in the robust FDI of uncertain nonlinear systems. However, due to the employed unknown-but bounded-uncertainty representation, the involved augmented state estimation problem turns out to be set-valued. This means that the estimation problem consists of constructing a *set of state values* that can be explained by both the uncertain model and the measurements. Set-valued estimation methods have received considerable attention in the recent control systems and state estimation literature. In the references (Chernousko, 2004) and (Milanese and Vicino, 1991) an excellent overview of work in this area is presented and (Kurzhanski and Veliov, 1993) contains a collection of papers that are related to this subject.

In this section, the basic principle of set-valued estimation is reviewed and first links to robust FDI are established. The starting point is the specification of the nonlinear set-valued estimation problem and the ideal solution to it. This is followed by an elaborate discussion of the extended set-valued estimation scheme which provides an approximate but also computationally tractable alternative to the ideal approach. This section does not provide a complete review of this field; it is rather intended to provide the basis for the subsequent investigations of robust FDI. For more comprehensive reviews in respect of nonlinear set-valued estimation, the reader is referred to the above cited literature.

4.2.1 Notation, Problem Statement, and Exact Solution

In the following, the problem of nonlinear set-valued estimation is specified and its exact solution by ideal nonlinear set-valued estimation is discussed. The basis for these considerations forms the i-th mode conditioned uncertain augmented state model $(\Sigma^{(i)}, \Omega^{(i)})$, $i \in \{0, \ldots, N\}$.

At first, some basic notation and fundamental definitions that are used throughout the remaining part of this chapter are introduced.

Definition 4.2 (Set of reachable states) *Let $\{u_\rho, y_\rho\}_0^k$ be a given I/O-sequence of the uncertain system $(\Sigma^{(i)}, \Omega^{(i)})$. Then,*

$$\mathbb{X}_k^{(i)} = \left\{ x_k^{(i)} \in \mathbb{R}^{n_x^{(i)}} \,\middle|\, x_0^{(i)}, \{u_\rho, y_\rho, w_\rho^{(i)}, v_\rho^{(i)}\}_0^k, \left(\Sigma^{(i)}, \Omega^{(i)}\right) \right\} \tag{4.10}$$

denotes the reachable set of augmented states $x_k^{(i)}$ at time k for the uncertain system $\Sigma^{(i)}$ with uncertainty inputs $\{w_\rho^{(i)}, v_\rho^{(i)}\}_0^k$ and initial condition $x_0^{(i)}$ satisfying the constraint $\Omega^{(i)}$ (with $u_k = u_\rho$, $w_k^{(i)} = w_\rho^{(i)}$, $v_k^{(i)} = v_\rho^{(i)}$ and $y_k = y_\rho$).

Regarding the mode conditioned system to be observed $(\Sigma^{(i)}, \Omega^{(i)})$ and the corresponding set of reachable states (4.10), the following assumption holds in the remaining part of this chapter.

Assumption 4.2 *It is assumed that the system $(\Sigma^{(i)}, \Omega^{(i)})$ is strictly verifiable on the time interval $[0, k]$.*

Thereby, the term of *strict verifiability* is chosen according to (Petersen and Savkin, 1999) and is defined as follows.

Definition 4.3 (Strict verifiability) *The system $(\Sigma^{(i)}, \Omega^{(i)})$ is said to be strictly verifiable on the interval $[0, k]$, if for any initial state $x_0^{(i)}$, any $\rho \in [0, k]$, any augmented uncertainty inputs $\{w_\rho^{(i)}, v_\rho^{(i)}\}_0^k$, and any fixed I/O-sequence $\{u_\rho, y_\rho\}_0^k$, the set of reachable augmented states $\mathbb{X}_k^{(i)}$ is bounded.*

Remark 4.3 *The assumption of a bounded set of reachable augmented states $\mathbb{X}_k^{(i)}$ and therefore of strict verifiability is a reasonable one if the uncertainty-sets $\hat{\mathbb{X}}_0^{(i)}$, $\mathbb{W}_k^{(i)}$, and $\mathbb{V}_k^{(i)}$ are uniformly bounded and if the system $(\Sigma^{(i)}, \Omega^{(i)})$ is (locally) uniformly observable under the knowledge of the exogenous inputs $w_k^{(i)}$ and $v_k^{(i)}$. For a more comprehensive discussion with respect to the relation between the boundedness of the state-set $\mathbb{X}_k^{(i)}$ and the uniform observability of $(\Sigma^{(i)}, \Omega^{(i)})$, the interested reader is directed to the references (Shamma and Tu, 1997) and (Shamma and Tu, 1999).*

On the basis of this setup, the problem of nonlinear set-valued augmented state estimation can be summarized as follows.

Problem 4.1 (Nonlinear Set-Valued Augmented State Estimation) *Let $\{u_\rho, y_\rho\}_0^k$, $k > M$, be a given I/O-sequence of the strictly verifiable system $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$, where M is a sufficiently large positive integer. Find the corresponding set $\mathbb{X}_k^{(i)}$ of all reachable augmented states $x_k^{(i)}$ at time k for the system $\Sigma^{(i)}$ with uncertainty inputs and initial conditions satisfying the constraint of $\Omega^{(i)}$.*

Remark 4.4 *Note that the restriction to strictly verifiable systems is generally inevitable since, if Assumption 4.2 does not hold, then it is unlikely that any reasonable conclusions can be obtained about the system model from measured data. In particular note that within the employed unknown-but-bounded uncertainty framework, if the strict verifiability condition is not satisfied, the model may be such that any I/O-sequence $\{u_\rho, y_\rho\}_0^k$ is possible.*

As in conventional nonlinear state estimation, there are also various ways to address the set-valued state estimation problem. Prior to turning to the concrete realization of the estimator employed in our subsequent FDI considerations, let us first glance at the ideal nonlinear set-valued estimator (NSVE) which determines the set of reachable states exactly. This is preeminently useful since it allows a comparison with the subsequently investigated approximate approach to NSVE.

The calculation of the ideal NSVE is performed recursively and consists of propagating estimated state-sets from one sampling instant to the next taking into account the system dynamics, the measured I/O-sequence and the uncertainty-model. The recursive deduction of the reachable set of states $\mathbb{X}_k^{(i)}$ is basically done in three steps that are summarized in terms of the following algorithm.

Algorithm 4.1 (Ideal Nonlinear Set-Valued Estimator (NSVE)) *Suppose* $\{u_\rho, y_\rho\}_0^k$, $k > M$, *to be a given I/O-sequence of the strictly verifiable system* $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ *and suppose* M *to be sufficiently large. Then, the ideal nonlinear set-valued estimator determines the set of reachable states* $\mathbb{X}_k^{(i)}$ *exactly as*

$$\mathrm{NSVE}\Big(\left(\Sigma^{(i)}, \Omega^{(i)}\right), \{u_\rho, y_\rho\}_0^k\Big) = \mathbb{X}_k^{(i)}. \tag{4.11}$$

The operator $\mathrm{NSVE}(\cdot)$ *comprises the following three computational steps that are carried out recursively over the sequence* $\rho \in [0, \ldots, k]$*:*

$$\begin{aligned}
\mathbb{X}_{\rho|\rho-1}^{(i)} &= \Pi\big(f^{(i)}, \mathbb{X}_{\rho-1}^{(i)}, \mathbb{W}_{\rho-1}^{(i)}, u_{\rho-1}\big) && \text{(4.12a)}\\
&= \left\{ x_\rho^{(i)} \in \mathbb{R}^{n_x^{(i)}} \;\middle|\; x_\rho^{(i)} = f^{(i)}\big(x_{\rho-1}^{(i)}, u_{\rho-1}, w_{\rho-1}^{(i)}\big), u_{\rho-1}, x_{\rho-1}^{(i)} \in \mathbb{X}_{\rho-1}^{(i)}, w_{\rho-1}^{(i)} \in \mathbb{W}_{\rho-1}^{(i)} \right\}\\
\bar{\mathbb{X}}_\rho^{(i)} &= \Phi_1\big(h^{(i)}, y_\rho, \mathbb{V}_\rho^{(i)}\big) && \text{(4.12b)}\\
&= \left\{ x_\rho^{(i)} \in \mathbb{R}^{n_x^{(i)}} \;\middle|\; y_\rho = h^{(i)}(x_\rho^{(i)}, u_\rho, v_\rho^{(i)}), u_\rho, y_\rho, v_\rho^{(i)} \in \mathbb{V}_\rho^{(i)} \right\}\\
\mathbb{X}_\rho^{(i)} &= \Phi_2\big(\mathbb{X}_{\rho|\rho-1}^{(i)}, \bar{\mathbb{X}}_\rho^{(i)}\big) && \text{(4.12c)}\\
&= \mathbb{X}_{\rho|\rho-1}^{(i)} \cap \bar{\mathbb{X}}_\rho^{(i)} \quad .
\end{aligned}$$

The three computation-steps that are executed by Algorithm 4.1 describe the reconstruction of two distinct state-sets and their intersection. The first step (4.12a) determines the state-set that is reachable through the model $f^{(i)}(\cdot)$ from the control input $u_{\rho-1}$, the uncertainty set $\mathbb{W}_{\rho-1}^{(i)}$, and the previously computed state-set estimate $\mathbb{X}_{\rho-1}^{(i)}$. The set computed in this manner is referred to as the predicted state-set $\mathbb{X}_{\rho|\rho-1}^{(i)}$. The second step (4.12b) determines the set of states $\bar{\mathbb{X}}_\rho^{(i)}$ (measured state-set) being reachable by the measurement y_ρ. In the third step (4.12c), the intersection of these two sets is formed yielding the state-set estimate $\hat{\mathbb{X}}_\rho^{(i)}$. This contains only those states which are both reachable and measurable. After $k > M$ iterations, with M being sufficiently large, the ideal and guaranteed state-set estimate $\mathbb{X}_k^{(i)}$ is gained. The steps (4.12a)-(4.12c) are each denoted by using operators, the prediction operator $\Pi(\cdot)$, the measurement operator $\Phi_1(\cdot)$, and the intersection operator $\Phi_2(\cdot)$. The algorithm's computation steps are graphically illustrated in Figure 4.7 for an exemplary second order system with a single output.

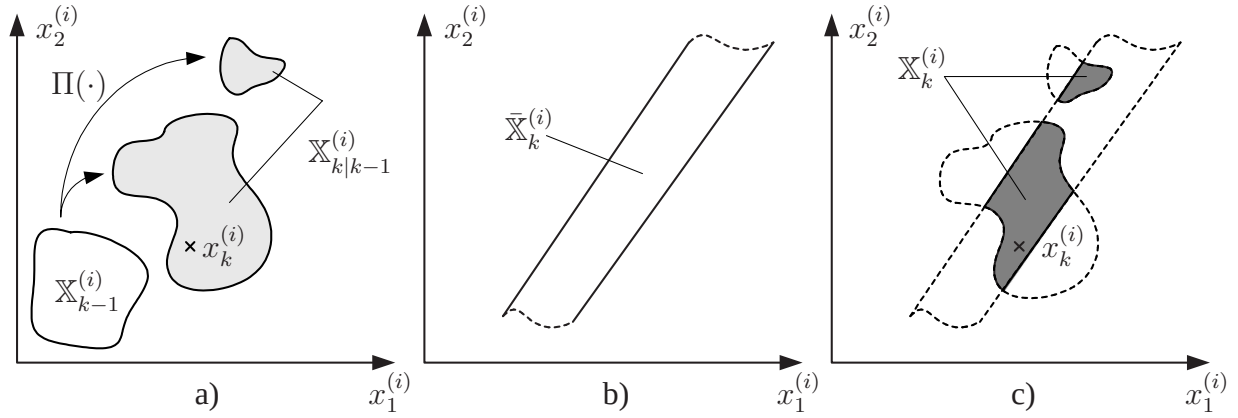


Figure 4.2: Graphical illustration of the NSVE computation steps, a) predicted state-set, b) measured state-set, and c) corrected state-set during set-valued estimation of an exemplary second order system with single output.

Remark 4.5 *Assuming that* $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ *is* M*-locally uniformly observable, which also implies the supposed strict verifiability of the system (see Remark 4.2), an adequate choice guaranteeing* M *to be sufficiently large is* $M \geq n_x^{(i)}$.

Regarding Algorithm 4.1 and the set of reachable states $\mathbb{X}_k^{(i)}$, the following property can be concluded.

Lemma 4.2 (Guaranty of the NSVE) *Suppose* $\left\{u_\rho, y_\rho\right\}_0^k$, $k > M$, *to be a given I/O-sequence of the strictly verifiable system* $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ *and suppose* M *to be sufficiently large. Then, the set of reachable states* $\mathbb{X}_k^{(i)}$ *as determined by Algorithm 4.1 is guaranteed to include the real state* $x_k^{(i)}$ *for all times, i.e.,*

$$x_k^{(i)} \in \mathbb{X}_k^{(i)}, \ \forall\, k. \tag{4.13}$$

Therefore, the ideal nonlinear set-valued estimation algorithm and the resulting set $\mathbb{X}_k^{(i)}$ *are said to be guaranteed.*

Proof. The proof of this lemma is trivial since it directly follows from Assumption 4.2 and from Definition 4.2. ■

Algorithm 4.1 gives a guaranteed and, under certain conditions, exact solution to the above specified nonlinear set-valued (augmented state) estimation problem. Unfortunately, the solution of Algorithm 4.1 is, in general, computationally intractable wherefore in practical applications, approximate NSVE schemes have to be employed.

In the following subsection, different approaches to approximate NSVE are discussed. The scheme of extended set-valued estimation is extensively reviewed and is related to the ideal set-valued estimator (4.11).

4.2.2 Extended Set-Valued Estimation

An exact computational solution of the nonlinear set-valued estimation problem is unfortunately intractable. To remedy this problem, a variety of approximate set-valued estimation schemes have been proposed in the literature. These linear and nonlinear estimation schemes basically distinguish in their utilized type of set-representation for approximating the ideal set estimates (4.12a)-(4.12c) and the uncertainty sets (4.4). The two most commonly encountered approaches to (outer) bounding-set approximation are using polytopes or ellipsoids to describe the uncertainty sets and the set estimates. Polytope methods are popular because, for linear systems, calculations can be made quickly and easily using linear programming (Chisci *et al.*, 1996; Kieffer *et al.*, 1998; Alamo *et al.*, 2003; Alamo *et al.*, 2005). Ellipsoid methods, however, are often desirable because they are capable to give a much simpler, nevertheless very effective set-representation as compared to the polytope methods (Shamma and Tu, 1997; Garulli and Vicino, 2001; Polyak *et al.*, 2004). Another advantage of using ellipsoids is that these are insightful because of their analogy to the covariance in the stochastic methods.

Most of current set-valued estimation approaches are primarily derived for linear systems. Extensions to nonlinear problems are suggested in (Shamma and Tu, 1997; Tsakalis and Song, 1994; Jaulin and Walter, 1993). However, these methods are only limited applicable, which is particularly due to their high computational expense. In (Scholte and Campbell, 2002) an ellipsoidal approach to NSVE is proposed which on the one hand applies to a wide class of real-time set-valued estimation problems and on the other hand closely relates to the well known EKF (see Section 3.5.3).

In this thesis the ellipsoidal approach to set-approximation/NSVE is employed and the *extended set-valued estimation (ESVE)* scheme as firstly proposed in (Scholte and Campbell, 2002) is utilized. The ESVE is essentially an extension of the linear estimation scheme provided by (Schweppe, 1968) to the nonlinear case and also closely relates to the recursive set-membership state estimation scheme proposed by (Bertsekas and Rhodes, 1971). Besides the generality and the relations to the EKF, the ESVE has also shown to be computationally efficient and to give non-conservative state-set estimates. Beyond these advantageous properties, the convergence of the ESVE has been extensively studied (Scholte and Campbell, 2003). Hence, the ESVE provides a solid basis for our subsequent robust FDI considerations.

In the next subsection, the ESVE algorithm is introduced by means of the i-th mode-conditioned uncertain system $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$. Important properties of the ESVE are reviewed and a simple example illustrates the estimation principle. Prior to turning to the concrete algorithm realization, first some basic notation and definitions are introduced.

4.2.2.1 Notation and Basic Definitions

With regard to the employed estimation framework, first the term of the *ellipsoid* is introduced by the following definition.

Definition 4.4 (Ellipsoid) *An ellipsoid $\mathcal{E}(\cdot)$ is given by the set*

$$\mathcal{E}(\hat{s}, S) := \left\{ s \in \mathbb{R}^{n_s} \,\middle|\, (s-\hat{s})^T S^{-1} (s-\hat{s}) \leq 1 \right\} \tag{4.14}$$

where $\hat{s}$ is the center, s is any point within the ellipsoid, and S is a positive definite matrix describing the ellipsoid's shape.

In view of outer set-approximations used later that utilize ellipsoids (4.14), another definition shall be introduced.

Definition 4.5 (Complete (and guaranteed) ellipsoidal approximation) *Suppose $\mathbb{S}$ to denote a compact set of variables s which has to be approximated by an ellipsoid* (4.14)*. Then, the ellipsoid* (4.14) *is said to give a complete approximation of $\mathbb{S}$, if*

$$\mathcal{E}(\hat{s}, S) \supseteq \mathbb{S}, \ \forall\, s. \tag{4.15a}$$

Furthermore, the above completeness property implies (4.14) *to determine a guaranteed approximation, i.e., it implies*

$$s \in \mathcal{E}(\hat{s}, S)), \ \forall\, s. \tag{4.15b}$$

It is clear that a complete set-approximation is always implied to be guaranteed, i.e., $\mathcal{E}(\hat{s}, S) \supseteq \mathbb{S} \Rightarrow s \in \mathcal{E}(\hat{s}, S)$ for all s. Of course, the reverse does not hold. Figure 4.3 illustrates a complete and a guaranteed approximation of an exemplary set $\mathbb{S}$ by two different ellipsoids (4.14).

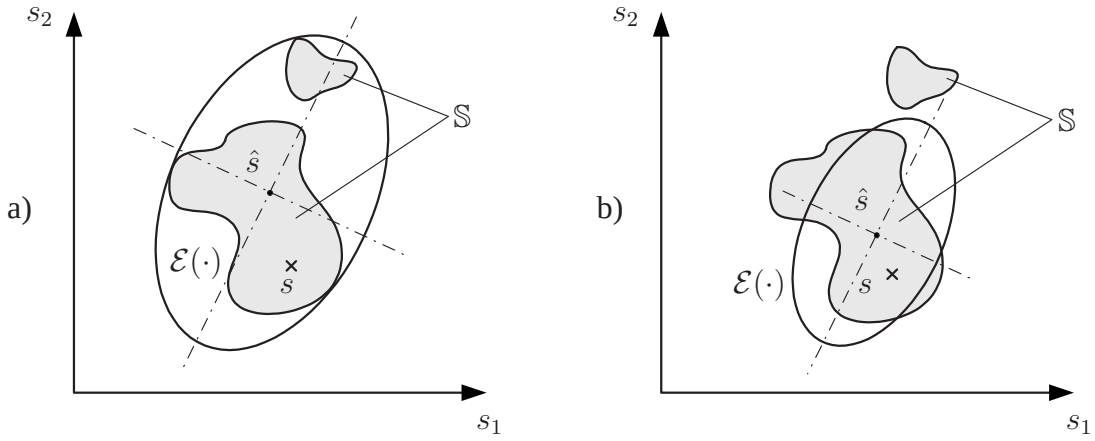


Figure 4.3: a) Complete and b) incomplete but guaranteed outer ellipsoidal bounding-set approximations and the true set to be approximated (gray area).

4.2.2.2 Extended Set-Valued Estimator – Algorithm Summary

In the following, the approximate set-valued augmented state estimation of the system $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ is considered. However, due to the employed ellipsoidal estimation approach, the uncertainty model $\Omega^{(i)}$ has to be replaced by the following constraint

$$\Omega_{\mathcal{E}}^{(i)} : \Big\{ x_0^{(i)} \in \mathcal{E}\big(\hat{x}_0^{(i)}, P_0^{(i)}\big),\ w_k^{(i)} \in \mathcal{E}\big(0, Q_k^{(i)}\big),\ v_k^{(i)} \in \mathcal{E}\big(0, R_k^{(i)}\big),\ \forall\, k, \tag{4.16}$$

where each bounding set is described by an ellipsoid (4.14). Regarding $\Omega_{\mathcal{E}}^{(i)}$, the following assumption holds:

Assumption 4.3 *The outer ellipsoidal uncertainty model $\Omega_{\mathcal{E}}^{(i)}$ is complete, i.e., $\Omega_{\mathcal{E}}^{(i)} \supseteq \Omega^{(i)}$ holds for all times k.*

ESVE is performed recursively and tends to determine an outer ellipsoidal state-set estimate with a possibly small volume (Scholte and Campbell, 2003). This is done by propagating the state-set estimate from one sampling instant to the next, taking into account the system dynamics, the control input, the measurement and the ellipsoidal uncertainty bounds. The ESVE computation steps are summarized in the following algorithm.

Algorithm 4.2 (Extended Set-Valued Estimator (ESVE)) *Let $\left\{u_\rho, y_\rho\right\}_0^k$, $k > M$, be a given I/O-sequence of the strictly verifiable system $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ and suppose M to be sufficiently large. Then, the* ESVE *determines the outer ellipsoidal estimate $\hat{\mathbb{X}}_k^{(i)}$ of the set of reachable states $\mathbb{X}_k^{(i)}$ as*

$$\mathrm{ESVE}\Big(\big(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\big), \left\{u_\rho, y_\rho\right\}_0^k\Big) = \hat{\mathbb{X}}_k^{(i)}. \tag{4.17}$$

Thereby, the operator $\mathrm{ESVE}(\cdot)$ *comprises the following computational steps being carried out recursively over the sequence $\rho \in [0, \ldots, k]$:*

1. Prediction step:

$$\tilde{Q}_{\rho-1}^{(i)} = G_{\rho-1}^{(i)} \frac{Q_{\rho-1}^{(i)}}{\beta_Q^{(i)}} G_{\rho-1}^{(i)T} + \frac{\bar{Q}_{\rho-1}^{(i)}}{1-\beta_Q^{(i)}} \tag{4.18a}$$

$$\hat{x}_{\rho|\rho-1}^{(i)} = f^{(i)}\big(\hat{x}_{\rho-1}^{(i)}, u_{\rho-1}, 0\big) \tag{4.18b}$$

$$P_{\rho|\rho-1}^{(i)} = A_\rho^{(i)} \frac{P_{\rho-1}^{(i)}}{1-\beta_Q^{(i)}} A_\rho^{(i)T} + \frac{\tilde{Q}_{\rho-1}^{(i)}}{\beta_Q^{(i)}} \tag{4.18c}$$

2. Correction step:

$$\tilde{R}_{\rho}^{(i)} = H_{\rho}^{(i)} \frac{R_{\rho}^{(i)}}{\beta_R^{(i)}} H_{\rho}^{(i)T} + \frac{\bar{R}_{\rho}^{(i)}}{1-\beta_R^{(i)}} \tag{4.19a}$$

$$\Lambda_{\rho}^{(i)}\big(\beta_{\rho}^{(i)}\big) = C_{\rho}^{(i)} \frac{P_{\rho|\rho-1}^{(i)}}{1-\beta_{\rho}^{(i)}} C_{\rho}^{(i)T} + \frac{\tilde{R}_{\rho}^{(i)}}{\beta_{\rho}^{(i)}} \tag{4.19b}$$

$$\bar{P}_{\rho}^{(i)} = \frac{P_{\rho|\rho-1}^{(i)}}{1-\beta_{\rho}^{(i)}} \left(I - C_{\rho}^{(i)T} \Big(\Lambda_{\rho}^{(i)}\big(\beta_{\rho}^{(i)}\big) \Big)^{-1} C_{\rho}^{(i)} \frac{P_{\rho|\rho-1}^{(i)}}{1-\beta_{\rho}^{(i)}} \right) \tag{4.19c}$$

$$\beta_{\rho}^{\star(i)} = \underset{\beta_{\rho}^{(i)} \in [0,1]}{\arg\min} \det\Big(\bar{P}_{\rho}^{(i)}\big(\beta_{\rho}^{(i)}\big) \Big) \tag{4.19d}$$

$$\eta_{\rho}^{(i)} = \Big(y_{\rho} - h^{(i)}\big(\hat{x}_{\rho|\rho-1}^{(i)}, u_{\rho}, 0\big) \Big)^{T} \Big(\Lambda_{\rho}^{(i)}(\beta_{\rho}^{\star(i)}) \Big)^{-1} \Big(y_{\rho} - h^{(i)}\big(\hat{x}_{\rho|\rho-1}^{(i)}, u_{\rho}, 0\big) \Big) \tag{4.19e}$$

$$\hat{x}_{\rho}^{(i)} = \hat{x}_{\rho|\rho-1}^{(i)} + \frac{P_{\rho|\rho-1}^{(i)}}{1-\beta_{\rho}^{\star(i)}} C_{\rho}^{(i)T} \Big(\Lambda_{\rho}^{(i)}\big(\beta_{\rho}^{\star(i)}\big) \Big)^{-1} \Big(y_{\rho} - h^{(i)}\big(\hat{x}_{\rho|\rho-1}^{(i)}, u_{\rho}, 0\big) \Big) \tag{4.19f}$$

$$P_{\rho}^{(i)} = (1-\eta_{\rho}^{(i)}) \bar{P}_{\rho}^{(i)}. \tag{4.19g}$$

Thereby, the utilized time-dependent matrices $A_{\rho}^{(i)}$, $G_{\rho}^{(i)}$, $C_{\rho}^{(i)}$, and $H_{\rho}^{(i)}$ denote the following Jacobians:

$$A_{\rho}^{(i)} = \left.\frac{\partial f^{(i)}}{\partial x^{(i)}}\right|_{(\hat{x}_{\rho-1}^{(i)}, u_{\rho-1}, 0)}, G_{\rho}^{(i)} = \left.\frac{\partial f^{(i)}}{\partial w^{(i)}}\right|_{(\cdot)}, C_{\rho}^{(i)} = \left.\frac{\partial h^{(i)}}{\partial x^{(i)}}\right|_{(\hat{x}_{\rho|\rho-1}^{(i)}, u_{\rho}, 0)}, H_{\rho}^{(i)} = \left.\frac{\partial h^{(i)}}{\partial v^{(i)}}\right|_{(\cdot)}.$$

After k iterations, the ellipsoidal estimate of the reachable state-set is obtained according to the following cases:

$$\hat{\mathbb{X}}_k^{(i)} := \begin{cases} \mathcal{E}\big(\hat{x}_k^{(i)}, P_k^{(i)}\big) & \text{if } \eta_k^{(i)} < 1 \\ \hat{x}_k^{(i)} & \text{if } \eta_k^{(i)} = 1 \\ \emptyset & \text{if } \eta_k^{(i)} > 1 \end{cases}. \tag{4.20}$$

The prediction step (4.18a)-(4.18c) is physically the addition of two ellipsoids, of the noise ellipsoid $\mathcal{E}\big(0, \tilde{Q}_{k-1}^{(i)}\big)$ and the state uncertainty ellipsoid $\mathcal{E}\big(\hat{x}_{k-1}^{(i)}, P_{k-1}^{(i)}\big)$ rotated and scaled by the matrices $A_k^{(i)T}$ and $A_k^{(i)}$. In general, the addition of two ellipsoids has no closed form solution and therefore requires to be again bounded by an outer ellipsoid. Under the terms of Algorithm 4.2, this is given by the Minkowski-Sum $\mathcal{E}_M\big(\hat{x}_{k|k-1}^{(i)}, P_{k|k-1}^{(i)}, \beta_Q^{(i)}\big)$ (Ros *et al.*, 2002), where $\beta_Q^{(i)} \in [0,1]$ is a scalar which has to be optimized in order to find the smallest outer bound. The correction step (4.19a)-(4.19g) is the intersection of two sets, of the predicted state-ellipsoid $\mathcal{E}_M(\cdot)$ and the (degenerate) ellipsoid described by the output equation $\mathcal{E}\big(y_k, \tilde{R}_k^{(i)}\big)$. The outer bounding ellipsoid of this intersection is given as $\mathcal{E}_I\big(\hat{x}_k^{(i)}, P_k^{(i)}, \beta_k^{(i)}\big)$ with free (to be optimized) parameter $\beta_k^{(i)} \in [0,1]$. These ESVE computation steps are illustrated by Figure 4.4 for an exemplary second order system with a single output. For a detailed consideration with respect to the derivation of the ESVE equations and the utilized ellipsoidal calculus, the interested reader is referred to (Schweppe, 1968) and (Ros *et al.*, 2002) respectively.

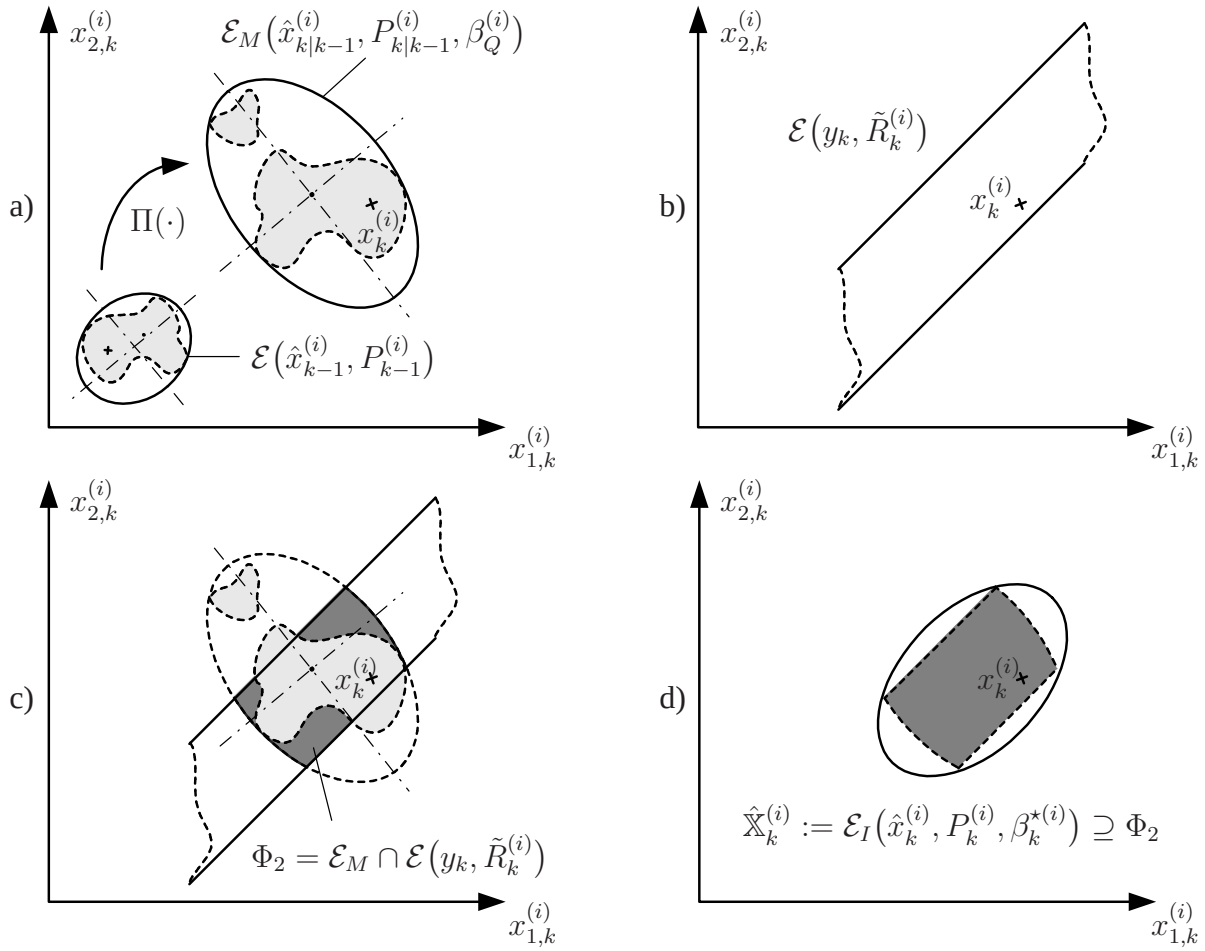


Figure 4.4: Illustration of the ESVE computation steps. a) Predicted state-set, b) measured state-set, c) intersection, and d) corrected state-ellipsoid for an exemplary second order system with single output.

As already mentioned, there are many similarities between the ESVE and the EKF. However, their physical interpretation is very different. Instead of propagating probability distributions, hard bounds are propagated in time that are guaranteed to contain the real state. Another distinctive feature of the ESVE is the way to approach the error introduced by the local linearization about the current state estimate. Unlike the EKF, the linearization errors are not neglected, rather these are factored into the existing exogenous inputs that are constrained by enhanced guaranteed bounds. The ESVE approach is shown in Figure 4.5 as compared to the EKF.

While the EKF determines a Gaussian probability distribution $\mathcal{N}\big(\hat{x}_k^{(i)}, P_k^{(i)}\big)$ of the state (with mean $\hat{x}_k^{(i)}$ and covariance $P_k^{(i)}$), the ESVE determines an ellipsoid $\mathcal{E}\big(\hat{x}_k^{(i)}, P_k^{(i)}\big)$ (with $\hat{x}_k^{(i)}$ defining the center and positive definite matrix $P_k^{(i)}$ describing the ellipsoid's shape and direction) which is guaranteed to contain the real state. The key to the ESVE for nonlinear systems is to bound the remainder (linearization error) and to combine this with the a priori uncertainty bounds (4.16) such that the bound is both non-conservative and amenable to on-line usage.

Let us now glance at the derivation of the bounding-ellipsoids that are guaranteed to capture both the model uncertainties (4.16) and the remainder. To simplify matters, the subsequent considera-

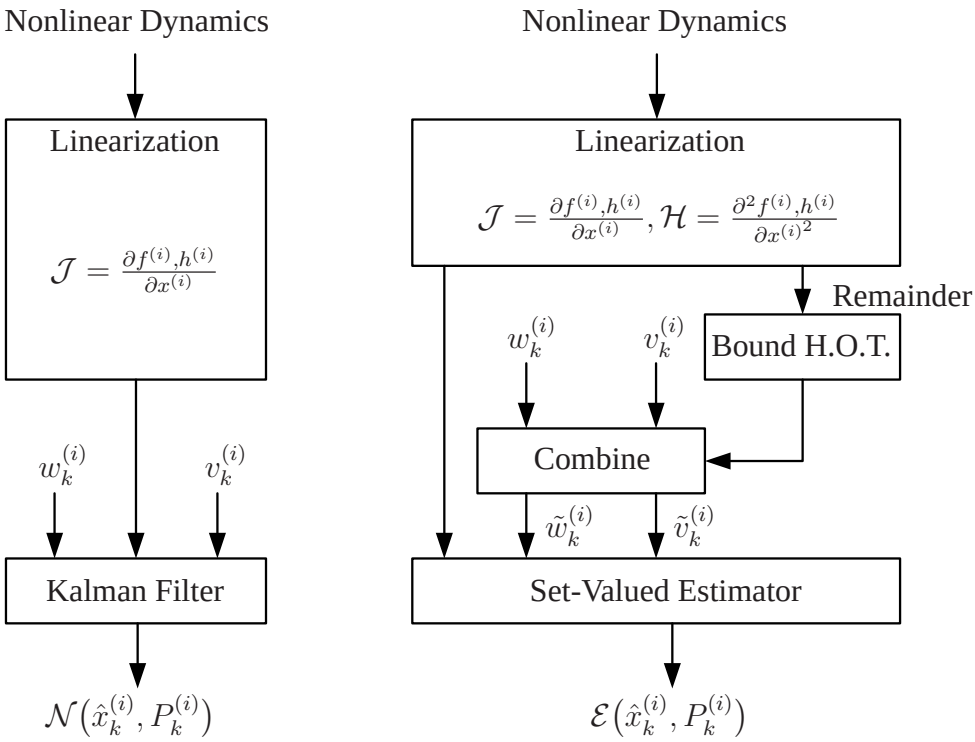


Figure 4.5: Simplified illustration of the EKF (left) and the ESVE (right) at each time step (utilized Jacobian matrices are denoted as $\mathcal{J}$, involved Hessian matrices are denoted as $\mathcal{H}$).

tions are based on the following simplification of (4.3):

$$x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}\big) + w_k^{(i)}, x_0^{(i)},\ k \geq 0 \tag{4.21a}$$

$$y_k = h^{(i)}\big(x_k^{(i)}\big) + v_k^{(i)}. \tag{4.21b}$$

Remark 4.6 *Note, that adding a deterministic control input u_k and considering the exogenous inputs $w_k^{(i)}$, $v_k^{(i)}$ to enter the system arbitrarily is a straightforward extension to the subsequent developments, but is left out for notational convenience.*

Linearizing the system equation (4.21a) around the ellipsoid's center $\hat{x}_k^{(i)}$ of the current state-set estimate $\mathcal{E}(\hat{x}_k^{(i)}, P_k^{(i)})$ yields

$$x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}\big)\Big|_{x_k^{(i)}=\hat{x}_k^{(i)}} + \frac{\partial f^{(i)}\big(x_k^{(i)}\big)}{\partial x^{(i)}}\Big|_{x_k^{(i)}=\hat{x}_k^{(i)}} \big(x_k^{(i)} - \hat{x}_k^{(i)}\big) + \text{H.O.T.} + w_k^{(i)}, \tag{4.22}$$

where H.O.T. refers to the higher order terms of the Taylor series expansion. Whereas the traditional EKF formulation ignores the higher order terms, the ESVE joins them on to the uncertainty $w_k^{(i)}$ in order to determine one common bound such that (4.22) can be rewritten as

$$x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}\big)\Big|_{x_k^{(i)}=\hat{x}_k^{(i)}} + \frac{\partial f^{(i)}\big(x_k^{(i)}\big)}{\partial x^{(i)}}\Big|_{x_k^{(i)}=\hat{x}_k^{(i)}} \big(x_k^{(i)} - \hat{x}_k^{(i)}\big) + \tilde{w}_k^{(i)}. \tag{4.23}$$

Thereby, $\tilde{w}_k^{(i)}$ is an uncertainty term bounding both the original model uncertainty $w_k^{(i)}$ and the linearization remainder. The extended uncertainty is outer bounded as follows

$$\tilde{w}_k^{(i)} \in \mathcal{E}\big(0, \tilde{Q}_k^{(i)}\big). \tag{4.24}$$

The output equation (4.21b) can be treated in a similar fashion such that the higher order terms of the nonlinear measurement are captured in a new uncertainty term $\tilde{v}_k^{(i)}$:

$$y_k^{(i)} = h^{(i)}\big(x_k^{(i)}\big)\Big|_{x_k^{(i)}=\hat{x}_k^{(i)}} + \frac{\partial h^{(i)}\big(x_k^{(i)}\big)}{\partial x^{(i)}}\bigg|_{x_k^{(i)}=\hat{x}_k^{(i)}} \big(x_k^{(i)} - \hat{x}_k^{(i)}\big) + \tilde{v}_k^{(i)}, \tag{4.25}$$

with

$$\tilde{v}_k^{(i)} \in \mathcal{E}\big(0, \tilde{R}_k^{(i)}\big). \tag{4.26}$$

Of course, the major challenge in bounding the linearization error is to determine the matrices $\tilde{Q}_k^{(i)}$ and $\tilde{R}_k^{(i)}$ respectively. In the following, the computation of $\tilde{Q}_k^{(i)}$ shall be outlined solely since the computation of $\tilde{R}_k^{(i)}$ is analogous.

Rewriting (4.23) with a remainder yields

$$x_{k+1}^{(i)} = f^{(i)}\big(x_k^{(i)}\big)\Big|_{x_k^{(i)}=\hat{x}_k^{(i)}} + \frac{\partial f^{(i)}\big(x_k^{(i)}\big)}{\partial x^{(i)}}\bigg|_{x_k^{(i)}=\hat{x}_k^{(i)}} \big(x_k^{(i)} - \hat{x}_k^{(i)}\big) + L^{(i)}\big(\hat{x}_k^{(i)}, x_k^{(i)}\big) + w_k^{(i)}, \tag{4.27}$$

where $L^{(i)}(\cdot)$ is the first-order Lagrange remainder term that is given element-wise as

$$L_\nu^{(i)}\big(\hat{x}_k^{(i)}, x_k^{(i)}\big) = \frac{1}{2}\big(x_k^{(i)} - \hat{x}_k^{(i)}\big)^T \underbrace{\frac{\partial^2 f_\nu^{(i)}\big(x_k^{(i)}\big)}{\partial {x_k^{(i)}}^2}\bigg|_{x_k^{(i)} \in \mathcal{E}(\hat{x}_k^{(i)}, P_k^{(i)})}}_{\mathcal{H}_\nu^{(i)}(x_k^{(i)})} \underbrace{\big(x_k^{(i)} - \hat{x}_k^{(i)}\big)}_{\Delta x_k^{(i)}}, \ \nu \in \{1, \dots, n_x^{(i)}\}. \tag{4.28}$$

A bound on the remainder (4.28) can be derived by solving the following quadratic optimization problem (Scholte and Campbell, 2002):

$$\overline{L}_{\nu,k}^{(i)} = \max_{\Delta x_k^{(i)} \in \mathcal{E}(0, P_k^{(i)}),\ x_k^{(i)} \in \mathcal{E}(\hat{x}_k^{(i)}, P_k^{(i)})} \left| \frac{1}{2}\, \Delta {x_k^{(i)}}^T \mathcal{H}_{\nu,k}^{(i)}(x_k^{(i)})\ \Delta x_k^{(i)} \right|. \tag{4.29}$$

The first-order Lagrange remainder $L^{(i)}(\cdot)$ is then bounded by the $n_x^{(i)}$ constraints describing a rectangular $n_x^{(i)}$-dimensional bounding-box:

$$\Big| L_\nu^{(i)}\big(\hat{x}_k^{(i)}, x_k^{(i)}\big) \Big| \leq \overline{L}_{\nu,k}^{(i)},\ \forall\, k,\ \forall\, \nu \in \{1, \dots, n_x^{(i)}\}. \tag{4.30}$$

Remark 4.7 *Unfortunately, the optimization problem* (4.29) *is generally non-convex and is therefore hard to solve in most cases. In (Scholte and Campbell, 2002) it is proposed to use interval mathematics to circumvent this problem - which, however, generally entails a more conservative*

bound on the remainder. For a comprehensive study of interval mathematics, the reader is referred to (Moore, 1966) and (Hansen, 1992). There are also several software packages for interval analysis[1].

In order to obtain an ellipsoidal bound being compatible to our utilized uncertainty description, the bounding box (4.30) has to be approximated by a complete outer ellipsoid as

$$L^{(i)}\big(\hat{x}_k^{(i)}, x_k^{(i)}\big) \in \mathcal{E}\left(0, \bar{Q}_k^{(i)}\right), \ \forall\, k. \tag{4.31}$$

Employing the results of (Ros *et al.*, 2002), the positive definite matrix $\bar{Q}_k^{(i)}$ can be computed as follows:

$$\bar{Q}_k^{(i)} = \frac{1}{n_x^{(i)}} \left[\text{diag}\left(\overline{L}_k^{(i)}\right)\right]^{-2}, \ \ \overline{L}_k^{(i)} = \left[\overline{L}_{1,k}^{(i)}, \ldots, \overline{L}_{n_x^{(i)},k}^{(i)}\right]^T. \tag{4.32}$$

The combined uncertainty bound including both the model uncertainty and the remainder can then be found by computing the Minkowski-Sum and bounding the respective ellipsoid, i.e.,

$$\mathcal{E}\big(0, \tilde{Q}_k^{(i)}\big) = \mathcal{E}_M\Big(\mathcal{E}\big(0, \bar{Q}_k^{(i)}\big), \mathcal{E}\big(0, Q_k^{(i)}\big), \beta_Q^{(i)}\Big). \tag{4.33}$$

Following again (Ros *et al.*, 2002), the matrix $\tilde{Q}_k^{(i)}$ determining the bounding ellipsoid (4.33) is given as

$$\tilde{Q}_k^{(i)} = \frac{\bar{Q}_k^{(i)}}{1-\beta_Q^{(i)}} + \frac{Q_k^{(i)}}{\beta_Q^{(i)}}, \ \ \beta_Q^{(i)} \in [0,1], \tag{4.34}$$

where $\beta_Q^{(i)}$ is a free parameter which can be optimized in an effort to find the smallest ellipsoid (4.33). For more continuative investigations of the above employed ellipsoidal calculus, the interested reader is directed to the references (Ros *et al.*, 2002), (Chernousko, 2004), and (Kurzhanski and Vályi, 1997).

The outer ellipsoid which bounds the combined uncertainty of the output equation (4.21b) is computed in a similar fashion, thus is omitted to be outlined explicitly. In analogy to (4.33) and (4.34), this is given as

$$\mathcal{E}\big(0, \tilde{R}_k^{(i)}\big) \text{ with } \tilde{R}_k^{(i)} = \frac{\bar{R}_k^{(i)}}{1-\beta_R^{(i)}} + \frac{R_k^{(i)}}{\beta_R^{(i)}}, \ \beta_R^{(i)} \in [0,1]. \tag{4.35}$$

Remark 4.8 *Note that if* $n_w^{(i)} = n_x^{(i)}$ *and* $n_v^{(i)} = n_y$*, then* $\beta_Q^{(i)} = \frac{n_w^{(i)}}{n_x^{(i)}+n_w^{(i)}}$ *and* $\beta_R^{(i)} = \frac{n_v^{(i)}}{n_y^{(i)}+n_v^{(i)}}$ *determine the optimal choice of the free parameters* $\beta_Q^{(i)}$ *and* $\beta_R^{(i)}$ *(see reference (Ros* et al.*, 2002)).*

[1] This work employs the free Interval Arithmetic Toolbox for Matlab provided by J. Zemke being online available at: `http://www.ti3.tu-harburg.de/~zemke/b4m/index.html`.

Example 4.1 *In order to gain insight into how the ESVE algorithm functions at each time step, this is exemplified by means of the Van der Pol oscillator system. The Van der Pol oscillator is assumed to operate fault-free in the mode m_0 and is described by the following uncertain discrete-time state space model*

$$\Sigma^{(0)}_{VdP}: \begin{cases} x^{(0)}_{1,k+1} = x^{(0)}_{1,k} + dT x^{(0)}_{2,x},\ x^{(0)}_{1,0},\ k \geq 0 \\ x^{(0)}_{2,k+1} = x^{(0)}_{2,k} + dT\big(\epsilon\, x^{(0)}_{2,k}(1 - {x^{(0)}_{1,k}}^2) - x^{(0)}_{1,k} + w^{(0)}_k\big),\ x^{(0)}_{2,0}\,, \\ \quad y_k = x^{(0)}_{1,x} + v^{(0)}_k \end{cases} \tag{4.36a}$$

where ϵ is a parameter scaling the nonlinearity in the second state equation, and the sampling rate $dT = 0.05$. The initial states as well as the exogenous inputs are unknown-but-bounded by the following constraints: $\hat{x}^{(0)}_0 \in \mathcal{E}\big([1\ 4]^T, \mathrm{diag}([2\ 2]^T)\big)$, $w^{(0)}_k \in \mathcal{E}\big(0,1\big)$, and $v^{(0)}_k \in \mathcal{E}\big(0,0.01\big)$. The Hessians for the above system equations are

$$\mathcal{H}_1\big(x^{(0)}_k\big) = dT \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ \mathcal{H}_2\big(x^{(0)}_k\big) = -2dT\epsilon \begin{bmatrix} x^{(0)}_{2,k} & x^{(0)}_{1,k} \\ x^{(0)}_{1,k} & 0 \end{bmatrix}. \tag{4.36b}$$

Hence, the uncertainty due to the linearization is one-dimensional yielding the following remainder term

$$\overline{L}^{(0)}_{f,k} = \max_{\Delta x^{(0)}_k \in \mathcal{E}(0,P^{(0)}_k),\ x^{(0)}_k \in \mathcal{E}(\hat{x}^{(0)}_k,P^{(0)}_k)} \left| -dT\epsilon\, \Delta {x^{(0)}_k}^T \begin{bmatrix} x^{(0)}_{2,k} & x^{(0)}_{1,k} \\ x^{(0)}_{1,k} & 0 \end{bmatrix} \Delta x^{(0)}_k \right|. \tag{4.36c}$$

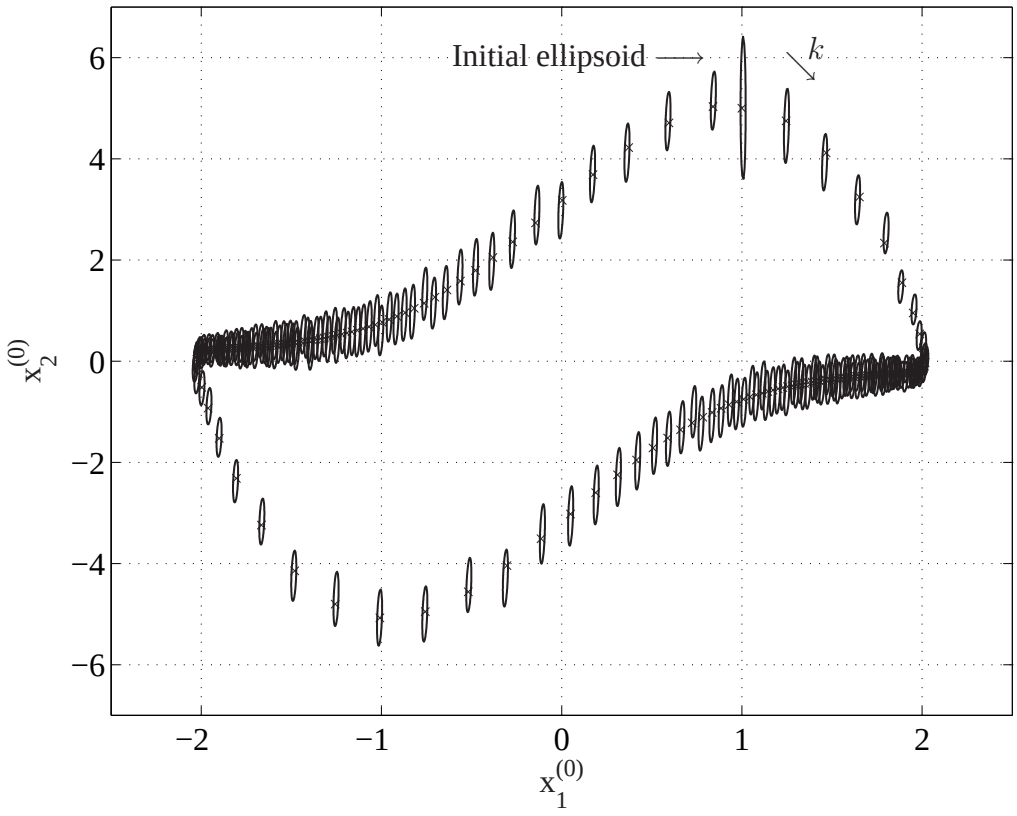


Figure 4.6: Actual state ("×"-symbol) and ellipsoidal state-set estimate (solid-lined ellipses) of the Van der Pol oscillator system using the uncertain model (4.36a).

Figure 4.6 shows the evolution of the state uncertainty ellipsoid as a function of time, over one period of the Van der Pol oscillator. The actual (real) state of the system $x_k^{(0)}$ is always contained within the estimated ellipsoidal state-set increasing and decreasing in size depending on the uncertainty (and state-dependent remainder). It emanates from (4.36c) *that the uncertainty which is due to linearization errors increases when $|x_{2,k}^{(0)}|$ increases; which is also shown in Figure 4.6.*

4.2.2.3 Properties of the ESVE

One of the most important features of the ESVE is its completeness and the resulting implication of $\hat{\mathbb{X}}_k^{(i)}$ to be guaranteed. This fundamental property is summarized by means of the following lemma.

Lemma 4.3 (Completeness of the ESVE) *Consider the ESVE described by Algorithm 4.2 and the corresponding problem setup. The ellipsoidal state-set estimate $\hat{\mathbb{X}}_k^{(i)}$ as gained by employing Algorithm 4.2 describes the set of reachable states $\mathbb{X}_k^{(i)}$ completely and furthermore, is guaranteed to include the real augmented state $x_k^{(i)}$, i.e.,*

$$\hat{\mathbb{X}}_k^{(i)} \supseteq \mathbb{X}_k^{(i)},\ x_k^{(i)} \in \mathbb{X}_k^{(i)},\ \forall\, k. \tag{4.37}$$

Therefore the ESVE as summarized in Algorithm 4.2 and the determined state-set estimate $\hat{\mathbb{X}}_k^{(i)}$ are said to be complete and guaranteed.

Proof. The proof of this lemma follows directly from the based estimation principle and the employed complete ellipsoidal bounding operations. ■

Remark 4.9 *Note that in order to determine non-conservative state-set estimates $\hat{\mathbb{X}}_k^{(i)} \cong \mathbb{X}_k^{(i)}$, over-approximation effects have to be kept as small as possible. Hence, the application of Algorithm 4.2 is usually restricted to weakly nonlinear systems. For a more detailed discussion in this respect, the interested reader is referred to (Tsakalis and Song, 1994).*

It remains to be seen, that Lemma 4.3 will play a key role in the subsequent FDI considerations. However, note that the relation (4.37) is a priori satisfied for any state-set estimate $\hat{\mathbb{X}}_k^{(i)}$ being unbounded. In such a case, an unbounded estimate $\hat{\mathbb{X}}_k^{(i)}$ would also give a complete but useless result. This is why another lemma addressing the convergence behavior of Algorithm 4.2 has to be introduced.

Lemma 4.4 (Non-divergence of the ESVE) *Consider the ESVE described by Algorithm 4.2 and the corresponding problem setup. Furthermore, assume the following:*

1. *The nonlinear functions $f^{(i)}(\cdot)$ and $h^{(i)}(\cdot)$ are sufficiently smooth, i.e., $A_k^{(i)}$, $G_k^{(i)}$, $C_k^{(i)}$, $H_k^{(i)}$ are uniformly bounded matrices and $A_k^{(i)^{-1}}$ exists for all k.*

2. *The uncertainties* $\tilde{w}_k^{(i)}$ *and* $\tilde{v}_k^{(i)}$ *are bounded, i.e.,* $\tilde{Q}_k^{(i)^{-1}} > 0$ *and* $\tilde{R}_k^{(i)^{-1}} > 0$.

3. *The system* $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ *is* M*-locally uniformly observable (under the knowledge of* $\mu_k^{(i)} = \left[u_k^T \; w_k^{(i)T} \; v_k^{(i)T}\right]^T$*), i.e., there exists an integer* $M \geq 1$ *such that*

$$\operatorname{rank} \frac{\partial}{\partial x^{(i)}} \left[\begin{array}{c} h^{(i)}\left(x^{(i)}, \mu_{k-M+1}^{(i)}\right) \\ h^{(i)}\left(\mu_{k-M+2}^{(i)}\right) \circ f^{(i)}\left(x^{(i)}, \mu_{k-M+1}^{(i)}\right) \\ \vdots \\ h^{(i)}\left(\mu_k^{(i)}\right) \circ f^{(i)}\left(\mu_{k-1}^{(i)}\right) \circ \cdots \circ f^{(i)}\left(x^{(i)}, \mu_{k-M+1}^{(i)}\right) \end{array} \right] \Bigg|_{x^{(i)}=x_{k-M+1}^{(i)}} = n_x^{(i)}. \quad (4.38)$$

4. *The initial state-set estimate is limited but not necessarily small, i.e., the matrix* $P_0^{(i)}$ *is uniformly bounded.*

Then, the ellipsoidal state-set estimate $\hat{\mathbb{X}}_k^{(i)}$ *is uniformly bounded for all times* k *and for all values* $\left\{\beta_Q^{(i)}, \beta_R^{(i)}, \beta_k^{(i)}\right\} \in [0, 1]$.

Proof. See (Scholte and Campbell, 2003) ■

In words, Lemma 4.4 states that the ESVE (4.17) is non-divergent whenever 1) the initial system state evolves within a not necessarily small but bounded set, 2) the system is M-locally uniformly observable given knowledge of all (exogenous) inputs, and 3) the uncertainties as well as linearization errors remain bounded. Therefore, as in the ideal NSVE case, $M \geq n_x^{(i)}$ is also a judicious choice in tuning Algorithm 4.2.

4.3 Robust FDI and Nonlinear Set-Valued Augmented State Estimation

This section establishes the relation between the afore reviewed NSVE approaches and the robust FDI with uncertain structured augmented state models. In the first instance, the link between model (mode) validation and robust FDI is created and the problem of robust FDI is specified. Based on ideal NSVE, a perfect but computationally intractable solution to robust FDI is presented which serves as a comparison for alternative solutions. By employing the afore investigated ESVE algorithm, a new and computationally tractable but approximate solution to robust FDI is introduced. Assuming a certain well-posedness of the underlying problem, this is proven to determine a robust FDI that is guaranteed to include the system's true mode at any time. Novel robust fault-detectability and -isolability conditions are derived disclosing both the reasonability of the underlying well-posedness assumption and a non-trivial FDI to be given as long as certain observability assumptions hold and the desired robustness/fault-sensitivity ratio is well-balanced.

4.3.1 Basic Setup – Ideal NSVE and Robust FDI

Prior to specifying the robust FDI problem and establishing the connection between mode validation and ideal nonlinear set-valued estimation, some basic definitions shall be introduced. The following definition forms the basis of the involved model validation problem.

Definition 4.6 *The I/O-sequence $\{u_\rho, y_\rho\}_0^k$ is said to be realizable with (denoted: r.w.) the uncertain augmented state model $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$, if there exist $\left(x_0^{(i)},\ \{w_\rho^{(i)}, v_\rho^{(i)}\}_0^k\right)$ satisfying conditions $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ with $u_k = u_\rho$, $w_k^{(i)} = w_\rho^{(i)}$, $v_k^{(i)} = v_\rho^{(i)}$ and $y_k = y_\rho$. This relation between the I/O-sequence and the model is denoted as*

$$\{u_\rho, y_\rho\}_0^k \text{ r.w. } \left(\Sigma^{(i)}, \Omega^{(i)}\right). \tag{4.39}$$

Definition 4.6 states that an observed system behavior can be explained by a certain mode m_i, if (4.39) holds. In other words, the mode m_i is valid as long as this condition applies, i.e., is invalid if not.

Due to the model uncertainty, it is quite possible that multiple modes are valid simultaneously, even though, as a matter of course, the real system is able to operate in one single mode only. To that effect, the following definition of the *set of valid modes* is introduced.

Definition 4.7 (Set of valid modes) *The set of valid modes $\mathbb{Z}_k^\star \subset \mathbb{Z}_?$ is defined according to the following cases:*

$$\mathbb{Z}_k^\star := \Big\{ m_0 \text{ if } \bar{\mathbb{Z}}_k^\star = \mathbb{Z};\ \bar{\mathbb{Z}}_k^\star \text{ if } \bar{\mathbb{Z}}_k^\star \subset \mathbb{Z};\ m_? \text{ if } \bar{\mathbb{Z}}_k^\star = \emptyset \Big\}. \tag{4.40}$$

Thereby, $\bar{\mathbb{Z}}_k^\star$ contains all modes m_i, $i \in \{0, \ldots, N\}$, with corresponding uncertain augmented state models $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ satisfying condition (4.39)*, i.e.,* $\bar{\mathbb{Z}}_k^\star := \left\{ m_i \in \mathbb{Z} \;\middle|\; \{u_\rho, y_\rho\}_0^k \text{ r.w. } \left(\Sigma^{(i)}, \Omega^{(i)}\right) \right\}$.

The set $\mathbb{Z}_k^\star$ is basically formed by the set of operating modes $\bar{\mathbb{Z}}_k^\star$ satisfying the afore investigated realizability relation. However, there are two operating modes that enforce a separate treatment, the fault-free mode m_0 and the unknown mode $m_?$. Due to the underlying state augmentation principle, all modes m_i satisfy the realizability relation (4.39) in the system's fault-free operation, hence, $\bar{\mathbb{Z}}_k^\star = \mathbb{Z}$ holds. This situation is ambiguous and can be only circumvented by assigning the mode m_0 by definition (first case of (4.40)). On the other hand, the situation may arise that the measured I/O-sequence is realizable by none of the modes m_i. In this case, the system has to operate in the unknown mode $m_?$; which can be simply reasoned by means of the completeness of the mode set $\mathbb{Z}_?$. The unknown mode situation is captured by the third case in (4.40).

Unfortunately in certain situations, the assignments of the modes m_0 and $m_?$ entail an error which may cause fault-modes to be classified as fault-free and unknown modes as known ones respectively; which is solely due to the modeling uncertainty. For the sake of tackling this problem, the following assumption supposing some kind of well-posedness of the underlying problem is made.

Assumption 4.4 (Well-posedness of the FDI problem) *In the following considerations, it is assumed that the considered FDI problem is well-posed in the sense that the assignments of the mode-set* (4.40) *apply exactly.*

Remark 4.10 *It remains to be seen in Section 4.3.2.2 that the above assumption is a reasonable one whenever the aimed robustness is in due proportion to the aimed fault sensitivity in regard to FDI.*

As a matter of fact, the set of valid modes $\mathbb{Z}_k^\star$ determines the best possible FDI that can be computed from the uncertain structured augmented state model and the measurements. Consequently, the link between mode validation and fault diagnosis is given and the problem of robust FDI can be stated as in the following definition.

Problem 4.2 (Robust FDI of uncertain systems) *Let $\{u_\rho, y_\rho\}_0^k$, $k > M$, be a given I/O-sequence of the uncertain structured augmented system $\mathcal{S}_\mathcal{U}$ (see equation* (4.9)*), where M is a sufficiently large positive integer. Then, the problem of robust FDI consists in determining mode-set estimate $\hat{\mathbb{Z}}_k$, which is non-trivial, i.e., $\hat{\mathbb{Z}}_k \cong \mathbb{Z}_k^\star$ and complete, i.e., $\hat{\mathbb{Z}}_k \supseteq \mathbb{Z}_k^\star$ for all times k.*

The estimated set of modes $\hat{\mathbb{Z}}_k$ determines a robust (or guaranteed) FDI since this includes the set of valid modes $\mathbb{Z}_k^\star$ completely. Hence, $\hat{\mathbb{Z}}_k$ inevitably includes the true operating mode $m_{i/?}$ at any time k. It is obvious that the estimated set $\hat{\mathbb{Z}}_k$ has to be as small as possible in order to determine a meaningful result - surely $\hat{\mathbb{Z}}_k = \mathbb{Z}$ would always give a robust but also trivial result of no significance.

Following Savkin and Petersen (Savkin and Petersen, 1995; Savkin and Petersen, 1997), a convenient method for verifying the realizability condition (4.39) is to employ set-valued estimation. The link between these two otherwise different problems can be seen from the following simple observation: If for a given I/O-sequence $\{u_\rho, y_\rho\}_0^k$, the corresponding set of reachable states $\mathbb{X}_k^{(i)}$ is empty, then the given measurement must be incompatible with the uncertain system model $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$. In this case, the uncertain system model and the corresponding mode m_i have been invalidated. This line of reasoning is summarized by the following proposition which establishes the connection between ideal NSVE and mode validation.

Proposition 4.1 *Suppose $\{u_\rho, y_\rho\}_0^k$, $k > M$, to be a given I/O-sequence of the system $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$. Furthermore, suppose that $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ is M-locally uniformly observable (under the knowledge of the exogenous inputs $w_k^{(i)}$ and $v_k^{(i)}$). Then, the I/O-sequence $\{u_\rho, y_\rho\}_0^k$ is realizable with the uncertain augmented state model $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$, if and only if*

$$\mathrm{NSVE}\Big(\left(\Sigma^{(i)}, \Omega^{(i)}\right), \{u_\rho, y_\rho\}_0^k\Big) = \mathbb{X}_k^{(i)} \neq \emptyset. \tag{4.41}$$

Proof. From the definition of the set $\mathbb{X}_k^{(i)}$ (see Definition 4.2) it follows that $\mathbb{X}_k^{(i)} \neq \emptyset$, if and only if there exist $\left(x_0^{(i)},\ \left\{w_\rho^{(i)}, v_\rho^{(i)}\right\}_0^k\right)$ satisfying the constraints $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$. Hence, the following equivalence applies: $\mathbb{X}_k^{(i)} \neq \emptyset \Leftrightarrow \exists\ \left(x_0^{(i)},\ \left\{w_\rho^{(i)}, v_\rho^{(i)}\right\}_0^k\right)$ such that $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ is satisfied. By Definition 4.6 this existence condition implies $\left\{u_\rho, y_\rho\right\}_0^k$ to be realizable with $\left(\Sigma^{(i)}, \Omega^{(i)}\right)$ - which finally proves the above proposition. ■

Proposition 4.1 states that the measured I/O-sequence is realizable with the uncertain augmented state model $(\Sigma^{(i)}, \Omega^{(i)})$, if and only if the ideal state-set estimate derived by Algorithm 4.1 is non-empty. In other words, the operating mode m_i as well as the corresponding uncertain augmented state model are valid as long as (4.41) holds. On the other hand, if $\mathbb{X}_k^{(i)} = \emptyset$, the mode m_i is invalidated. Consequently, the application of Proposition 4.1 to the set of valid modes (4.40) leads to the ideal solution of Problem 4.2. This statement shall be summarized by means of the following theorem.

Theorem 4.1 (Ideal solution to Problem 4.2) *Consider the Problem 4.2 to be given. Then, the estimated set of modes*

$$\hat{\mathbb{Z}}_k^\star := \left\{ m_0 \text{ if } \hat{\bar{\mathbb{Z}}}_k^\star = \mathbb{Z};\ \hat{\bar{\mathbb{Z}}}_k^\star \text{ if } \hat{\bar{\mathbb{Z}}}_k^\star \subset \mathbb{Z};\ m_? \text{ if } \hat{\bar{\mathbb{Z}}}_k^\star = \emptyset \right\}, \tag{4.42a}$$

with $\hat{\bar{\mathbb{Z}}}_k^\star := \left\{ m_i \in \mathbb{Z} \;\middle|\; \mathbb{X}_k^{(i)} \neq \emptyset \right\}$ *determines the ideal solution to the robust FDI Problem 4.1., i.e.,*

$$\hat{\mathbb{Z}}_k^\star = \mathbb{Z}_k^\star,\ \forall\ k. \tag{4.42b}$$

Proof. The proof of Theorem 4.1 follows directly from the combination of Proposition 4.1 and Definition 4.7. ■

4.3.2 Approximate Approach to Robust FDI Using the ESVE Algorithm

It is known from prior investigations that an exact solution to the nonlinear set-valued estimation problem is computationally intractable in most cases, hence condition (4.41) usually cannot be checked in practice. In order to gain a verifiable condition for a certain mode's validity/invalidity, we have to provide a link between mode validation and approximate set-valued estimation. Considering the afore introduced approximate ESVE scheme (Algorithm 4.2), this link emanates from Proposition 4.1 and can be summarized as follows:

Proposition 4.2 *Suppose* $\left\{u_\rho, y_\rho\right\}_0^k$, $k > M$, *to be a given I/O-sequence of the system* $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ *and suppose that this is* M*-locally uniformly observable (under the knowledge of the exogenous inputs* $w_k^{(i)}$ *and* $v_k^{(i)}$*). If the I/O-sequence* $\left\{u_\rho, y_\rho\right\}_0^k$ *is realizable with the uncertain augmented state model* $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$*, then*

$$\mathrm{ESVE}\Big(\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right), \left\{u_\rho, y_\rho\right\}_0^k\Big) = \hat{\mathbb{X}}_k^{(i)} \neq \emptyset, \tag{4.43a}$$

i.e., if

$$\mathrm{ESVE}\Big(\big(\Sigma^{(i)},\Omega_{\mathcal{E}}^{(i)}\big),\big\{u_\rho,y_\rho\big\}_0^k\Big)=\hat{\mathbb{X}}_k^{(i)}=\emptyset, \tag{4.43b}$$

then the I/O-sequence $\big\{u_\rho,y_\rho\big\}_0^k$ *is not realizable with the model* $\big(\Sigma^{(i)},\Omega_{\mathcal{E}}^{(i)}\big)$.

Proof. It follows from Proposition 4.1 that $\big\{u_\rho,y_\rho\big\}_0^k$ is realizable with $\big(\Sigma^{(i)},\Omega^{(i)}\big)$, if and only if $\mathbb{X}_k^{(i)}\neq\emptyset$. Since the employed ESVE is complete (see Lemma 4.3) and $\Omega_{\mathcal{E}}\supseteq\Omega$, it follows that $\hat{\mathbb{X}}_k^{(i)}\supseteq\mathbb{X}_k^{(i)}$ holds for all k. This implies $\mathbb{X}_k^{(i)}\neq\emptyset\Rightarrow\hat{\mathbb{X}}_k^{(i)}\neq\emptyset$ and $\hat{\mathbb{X}}_k^{(i)}=\emptyset\Rightarrow\mathbb{X}_k^{(i)}=\emptyset$ - which proves the first and the second part of this proposition respectively. ■

Remark 4.11 *From the consideration of the ESVE relation (4.19g), it is obvious that if* $\eta_k^{(i)}>1$, *then the matrix* $P_k^{(i)}$ *as well as the state uncertainty ellipsoid* $\hat{\mathbb{X}}_k^{(i)}$ *are not defined. Consequently, the ellipsoidal state-set estimate* $\hat{\mathbb{X}}_k^{(i)}$ *as gained by computing Algorithm 4.2 is indicated to be nonempty, if* $\eta_k^{(i)}\leq 1$ *and is indicated to be empty, if* $\eta_k^{(i)}>1$, *i.e.,*

$$\eta_k^{(i)}\leq 1\Rightarrow\hat{\mathbb{X}}_k^{(i)}\neq\emptyset,\ \eta_k^{(i)}>1\Rightarrow\hat{\mathbb{X}}_k^{(i)}=\emptyset. \tag{4.44}$$

By this means, the relations (4.43a) *and* (4.43b) *of Proposition 4.2 can be simply checked by verifying the inequalities* (4.44).

Proposition 4.2 states that a valid mode inherently leads to a nonempty ellipsoidal state-set estimate of the mode conditioned state-set, i.e., that an empty state-set estimate always identifies an invalid mode correctly. Compared to Proposition 4.1, Proposition 4.2 is practically checkable by verifying (4.44). However, it is non-bidirectional and may possibly lead to conservative results and thus, to a "late" recognition of a certain mode's invalidity. Both the non-bidirectionality and the conservativeness are due to over-approximation errors coming along with the outer ellipsoidal bounding operations and the linearizations that are performed in Algorithm 4.2 (see Figure 4.5). However, if we suppose again that Assumption 4.4 holds, then Proposition 4.2 can be applied bidirectionally and the following theorem can be stated.

Theorem 4.2 (Approximate solution to Problem 4.2) *Consider the Problem 4.2 to be given and suppose that it is well-posed according to Assumption 4.4. Then, the estimated set of modes*

$$\hat{\mathbb{Z}}_k:=\Big\{m_0\text{ if }\hat{\bar{\mathbb{Z}}}_k=\mathbb{Z};\ \hat{\bar{\mathbb{Z}}}_k\text{ if }\hat{\bar{\mathbb{Z}}}_k\subset\mathbb{Z};\ m_?\text{ if }\hat{\bar{\mathbb{Z}}}_k=\emptyset\Big\}, \tag{4.45a}$$

with $\hat{\bar{\mathbb{Z}}}_k:=\Big\{m_i\in\mathbb{Z}\ \Big|\ \hat{\mathbb{X}}_k^{(i)}\neq\emptyset\Big\}$, *determines an approximate but robust FDI according to Problem 4.2, i.e.,*

$$\hat{\mathbb{Z}}_k\supseteq\mathbb{Z}_k^\star,\ \forall\ k. \tag{4.45b}$$

Proof. From the combination of Definition 4.7 and the first relation of Proposition 4.2 it follows that $\hat{\bar{\mathbb{Z}}}_k\supseteq\bar{\mathbb{Z}}_k^\star$ holds for all k; which already proves condition (4.45b) to hold in the second case of

(4.45a). In order to prove the theorem also for the first and the second case of (4.45a), we have to apply Assumption 4.4 which allows a bidirectional application of Proposition 4.2. Together with Definition 4.7, this proves $\hat{\bar{\mathbb{Z}}}_k = \bar{\mathbb{Z}}_k^\star$ for all k in both cases, hence proves (4.45b) for the first and the third case of (4.45a) respectively. ■

If we suppose that Assumption 4.4 is satisfied, the estimated set of modes (4.45a) provides a correct, nontrivial, and computationally tractable solution to the underlying robust FDI problem. Prior to investigating the conditions by which Assumption 4.4 is a reasonable one, a simple strategy for determining the set (4.45a) under the terms of a non-switching environment shall be addressed briefly.

4.3.2.1 A Simple Robust FDI Scheme (Non-Switching Case)

The simplest way to compute the robust FDI (4.45a) is to instantiate a bank of mode-conditioned ESVEs and to operate them concurrently:

$$\left.\begin{array}{c} \mathrm{ESVE}\Big(\big(\Sigma^{(0)}, \Omega_{\mathcal{E}}^{(0)}\big),\ \{u_\rho, y_\rho\}_0^k\Big) \\ \vdots \\ \mathrm{ESVE}\Big(\big(\Sigma^{(N)}, \Omega_{\mathcal{E}}^{(N)}\big), \{u_\rho, y_\rho\}_0^k\Big) \end{array}\right\} = \left\{\hat{\mathbb{X}}_k^{(0)}, \ldots, \hat{\mathbb{X}}_k^{(N)}\right\} \Rightarrow \hat{\mathbb{Z}}_k. \tag{4.46}$$

As long as the considered system constantly operates in one particular mode during the complete FDI process (which excludes the FDI of intermittent faults and the FDI of faults occurring during the diagnosis process), the estimator bank (4.46) applies adequately. A more general scheme to robust FDI that is able to cope with switching FDI problems is provided in Section 4.4.

4.3.2.2 Conditions for a Meaningful FDI and Well-Posedness of the Problem

In the following, robust fault-detectability and -isolability conditions are derived. Provided that these conditions hold, the estimated set of modes (4.45a) is guaranteed to determine a unique FDI. By means of these conditions it is furthermore shown that the crucial well-posedness Assumption 4.4 is reasonable whenever the desired robustness is in due proportion to the desired fault-sensitivity of FDI.

Remark 4.12 (Notation) *In the subsequent propositions, theorems, and the corresponding proofs, some particular notation is employed. Thereby, the evaluated conditions for the detection/isolation of a certain mode m_i, denoted as $\mathcal{D}(m_i)$/$\mathcal{I}(m_i)$, are written on the right-hand side of these two expressions, i.e.,*

$$\mathcal{D}(m_i) : \text{fault detection condition}, \quad \mathcal{I}(m_i) : \text{fault isolation condition}.$$

Fault detection and isolation conditions that are effectively evaluated during the computation of the robust FDI (4.42a) *are additionally indicated by the subindex "FDI".*

In the first instance, a condition for robust fault-detectability is derived and finally summarized in form of Theorem 4.3. It basically states that under certain conditions, there is a guarantee that each of the considered fault-modes m_i, $i \in \{1,\dots,N\}$, is detected by a diagnosis function determining a robust FDI according to (4.45a). For the proof of this condition, the following proposition is required to be stated initially.

Proposition 4.3 *Let $\{u_\rho, y_\rho\}_0^k$, $k > M$ be a given I/O-sequence of the system $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ and suppose that $M = n_x^{(i)}$. Furthermore suppose that for $i \in \{1,\dots,N\}$, there exists a uniform upper bounding matrix $P_{max}^{(i)} > P_k^{(i)}$ for all times k, which uniformly bounds the state-set estimate*

$$\text{ESVE}\Big(\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right), \{u_\rho, y_\rho\}_0^k\Big) = \hat{\mathbb{X}}_k^{(i)}. \tag{4.47a}$$

Then, if

$$\left|\xi_{\nu,k}^{(i)}\right| > \left(\theta_{\nu,k}^{(i)} := \left|\hat{\xi}_{\nu,k}^{(i)}\right| - \sqrt{P_k^{(i)}\left(n_x+\nu, n_x+\nu\right)}\right) > 0,\ \nu \in \left\{1,\dots,n_\xi^{(i)}\right\}, \tag{4.47b}$$

the faulty operating mode m_i is guaranteed to be detected according to the following fault detection condition:

$$\mathcal{D}(m_i) : \left(\xi_k^{(i)} = \xi_{\mathcal{H}}^{(i)} := 0\right) \notin \hat{\mathbb{X}}_k^{(i)}. \tag{4.47c}$$

Proof. First note that the existence of a fault state satisfying (4.47b) requires the existence of a uniform upper bounding matrix $P_{\max}^{(i)}$. This is reasonable, if $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ is M-locally uniformly observable under the knowledge of the exogenous inputs $\left\{w_\rho^{(i)}, v_\rho^{(i)}\right\}_0^k$. Furthermore notice that the underlying ESVE approach implies the real state $x_k^{(i)}$ being always contained in $\hat{\mathbb{X}}_k^{(i)}$, i.e., $x_k^{(i)} \in \hat{\mathbb{X}}_k^{(i)} \neq \emptyset$ for all k. Hence, (4.47c) gives an adequate fault-detection condition. It follows from geometric considerations that (4.47c) is satisfied, if least one element $\xi_{\nu,k}^{(i)}$ of the real fault state satisfies condition (4.47b) - which means that the real fault-state's magnitude $\left|\xi_{\nu,k}^{(i)}\right|$ is larger than the (always positive) threshold $\theta_{\nu,k}^{(i)} > 0$ (see Figure 4.7). ■

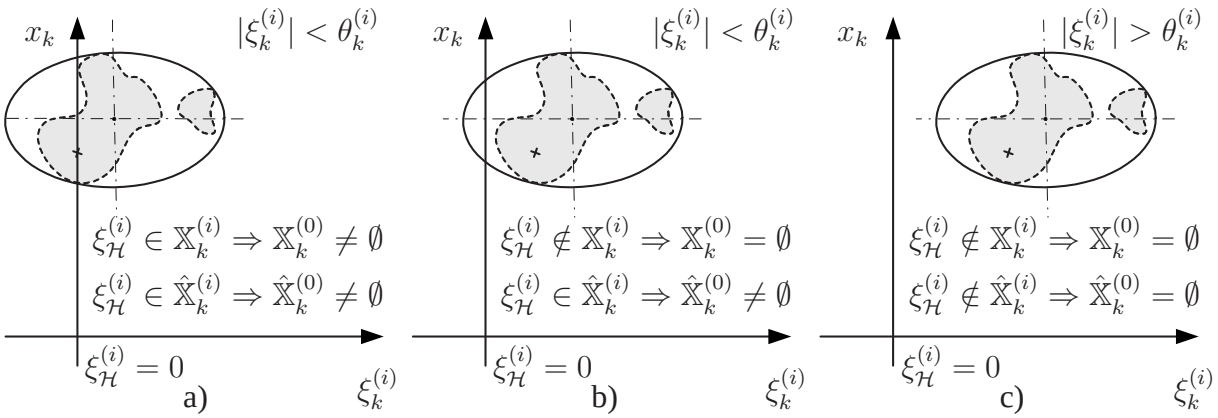


Figure 4.7: Graphical illustration of the ideal (gray area) and ellipsoidal i-th mode-conditioned augmented state-set estimate for the a) fault-free case (correctly identified), b) ill-posed problem of a faulty case (undetected by (4.45a)), and c) well-posed problem of a faulty case (detected by (4.45a)).

Proposition 4.3 states that a certain fault mode m_i is guaranteed to be detected, if the magnitude of the real fault-state exceeds the detection threshold (4.47b). By proving that condition (4.47c) is suitable to replace the virtually verified fault-detection condition (4.45a), the following theorem for the robust fault-detectability of Problem 4.2 can be stated.

Theorem 4.3 (Fault detection condition) *Let $\{u_\rho, y_\rho\}_0^k$, $k > M = n_x^{(i)}$, be a given I/O-sequence of the system $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$, $i \in \{0, \ldots, N\}$, and suppose that there exists a bounding matrix such that $P_{max}^{(i)} > P_k^{(i)}$ holds for all k. Then, if at least one element of the real fault-state $\xi_k^{(i)}$ satisfies condition* (4.47b)*, the estimated set of modes* (4.45a) *is guaranteed to exclude the fault-free operating mode m_0, i.e., the faulty mode m_i is guaranteed to be detected as*

$$\mathcal{D}_{\text{FDI}}(m_i) : \hat{\mathbb{X}}_k^{(0)} = \emptyset. \tag{4.48}$$

Proof. In order to prove the theorem, firstly a link between the virtually verified fault detection condition (4.48) and condition (4.47c) has to be established. Therefore, it shall be firstly glanced at

$$\text{ESVE}\Big(\left(\Sigma^{\star(i)}, \Omega_{\mathcal{E}}^{\star(i)}\right), \{u_\rho, y_\rho\}_0^k\Big) = \hat{\mathbb{X}}_k^{\star(i)} \neq \emptyset,\ \hat{\mathbb{X}}_k^{\star(i)} \subseteq \hat{\mathbb{X}}_k^{(i)}. \tag{4.49}$$

The ESVE (4.49) is conditioned on the mode m_i and is supposed to utilize the augmented state model $\Sigma^{\star(i)} = \Sigma \circ \Delta^{\star(i)}$ that contains the ideal (fictitious) exosystem $\Delta^{\star(i)}$ describing the i-th fault exactly. Due to the exactness of the exosystem $\Delta^{\star(i)}$, $\Omega_{\mathcal{E}}^{\star(i)} = \Omega_{\mathcal{E}}^{(0)}$ holds – which implies the following equivalence:

$$\mathcal{D}^{\star}(m_i) : \left(\xi_k^{(i)} = \xi_{\mathcal{H}}^{(i)} := 0\right) \notin \hat{\mathbb{X}}_k^{\star(i)} \ \Leftrightarrow\ \mathcal{D}_{\text{FDI}}(m_i). \tag{4.50}$$

Because $\hat{\mathbb{X}}_k^{(i)} \supseteq \hat{\mathbb{X}}_k^{\star(i)}$ holds for all k, we have $\mathcal{D}(m_i) \Rightarrow \mathcal{D}_{\text{FDI}}(m_i) \Leftrightarrow \mathcal{D}^{\star}(m_i)$. By this means, the fault-mode m_i is detected as $\mathcal{D}_{\text{FDI}}(m_i) : \hat{\mathbb{X}}_k^{(0)} = \emptyset$ as soon as (4.47c) is satisfied. Applying Proposition 4.3 finally completes the proof. ■

Theorem 4.3 states that a robust FDI function determining the set (4.45a) is guaranteed to detect each fault-mode correctly, if the mode-conditioned augmented system is observable (under the knowledge of the exogenous inputs) and, if relation (4.47b) is satisfied. Whereas the first condition directly relates to the property of nominal fault-detectability (see Theorem 3.1), the second condition identifies the inherent trade-off between achievable robustness and performance. Further discussions on this important result shall be outlined by means of Figure 4.7.

Figure 4.7 shows the ideal and the ellipsoidal augmented state-set estimates as assigned to the fault-mode m_i. Three different situations are illustrated which basically distinguish the considered degree of fault, i.e., the magnitude of the fault-state $\xi_k^{(i)}$. In the first sub-figure a), the system is exemplified to operate in the fault-free mode since the augmented state $x_k^{(i)}$ (illustrated by the $\times$-symbol) rests on the $\left(\xi_k^{(i)} = \xi_{\mathcal{H}}^{(i)} := 0\right)$-axis. Because both the ideal and the ellipsoidal augmented

state-set estimate include the real state $x_k^{(i)}$, no fault is detected by the corresponding FDI function and the fault-free mode is identified correctly. In contrast, Figure 4.7 b) illustrates a faulty operation of the system. Whereas the ideal FDI function using $\mathbb{X}_k^{(i)}$ detects the fault correctly, the FDI based on the approximate expression $\hat{\mathbb{X}}_k^{(i)}$ fails, since $\hat{\mathbb{X}}_k^{(i)}$ still includes a part of the $\left(\xi_k^{(i)} = \xi_{\mathcal{H}}^{(i)} := 0\right)$-axis. Hence, this is an example of an ill-posed FDI problem in which Assumption 4.4 is not reasonable and the bidirectional application of Proposition 4.2 leads to a wrong result that still diagnoses a fault-free operation of the system. A well-posed FDI problem is illustrated by the last sub-figure c). In this case, (4.47b) is satisfied and Assumption 4.4 is a reasonable one. Hence, the fault is detected by both the ideal and the approximate approach.

Following the same line of reasoning as in the detection case, a condition for robust fault-isolability can be derived similarly.

Proposition 4.4 *Let* $\left\{u_\rho, y_\rho\right\}_0^k$, $k > M = \max\limits_{(i,j)}(n_x^{(i,j)})$, *be a given I/O-sequence of the system* $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$. *Furthermore suppose that for* $(i \neq j) \in \{1, \ldots, N\}$, *there exists a uniform upper bounding matrix* $P_{max}^{(i,j)} > P_k^{(i,j)}$ *for all times* k *which uniformly bounds the state-set estimate*

$$\mathrm{ESVE}\Big(\left(\Sigma^{(i,j)}, \Omega_{\mathcal{E}}^{(i,j)}\right), \left\{u_\rho, y_\rho\right\}_0^k\Big) = \hat{\mathbb{X}}_k^{(i,j)}. \tag{4.51a}$$

Then, if

$$\left|\xi_{\nu,k}^{(i)}\right| > \left(\theta_{\nu,k}^{(i,j)} := \left|\hat{\xi}_{\nu,k}^{(i,j)}\right| - \sqrt{P_k^{(i,j)}\left(n_x+\nu, n_x+\nu\right)}\right) > 0,\ \nu \in \left\{1, \ldots, n_\xi^{(i)}\right\}, \tag{4.51b}$$

the faulty operating mode m_i *is guaranteed to be isolated from the mode* m_j *according to the following fault isolation condition:*

$$\mathcal{I}(m_i) : \left(\xi_k^{(i)} = \xi_{\mathcal{H}}^{(i)} := 0\right) \notin \hat{\mathbb{X}}_k^{(i,j)},\ \left(\xi_k^{(j)} = \xi_{\mathcal{H}}^{(j)} := 0\right) \in \hat{\mathbb{X}}_k^{(i,j)}. \tag{4.51c}$$

Proof. The proof is similar to the proof of Proposition 4.2. Note that the existence of a fault state satisfying (4.51b) requires the existence of $P_{\max}^{(i,j)}$; which is reasonable, if the augmented uncertain model $\left(\Sigma^{(i,j)}, \Omega_{\mathcal{E}}^{(i,j)}\right)$ is M-locally uniformly observable under the knowledge of $\left\{w_\rho^{(i,j)}, v_\rho^{(i,j)}\right\}_0^k$ (see Lemma 4.4). Furthermore notice that the underlying ESVE approach implies the real state $x_k^{(i,j)}$ to be always contained in $\hat{\mathbb{X}}_k^{(i,j)}$, i.e., $x_k^{(i,j)} \in \hat{\mathbb{X}}_k^{(i,j)} \neq \emptyset$ for all k. Hence, (4.51c) states an adequate condition for the isolation of m_i from m_j. Finally, geometric considerations show (4.51c) to be definitely satisfied as soon as at least one element $\xi_{\nu,k}^{(i)}$ of the real fault state satisfies condition (4.51b). ■

By means of Proposition 4.4, a condition for robust fault-isolability can be stated which is summarized by the following theorem.

Theorem 4.4 (Fault isolation condition) *Let* $\left\{u_\rho, y_\rho\right\}_0^k$, $k > M = \max\limits_{(i,j)}(n_x^{(i,j)})$ *be a given I/O-sequence of the system* $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ *and suppose that there exists a uniform bounding matrix* $P_{max}^{(i,j)}$

for any $(i \neq j) \in \{1, \ldots, N\}$ *such that* $P_{max}^{(i,j)} > P_k^{(i,j)}$ *holds for all times* k*. Then, if condition* (4.51b) *holds for all pairs of modes* $m_i \neq m_j \in \mathbb{Z}$*, the estimated set of modes* (4.45a) *is guaranteed to exclude all of the mismatched modes* m_j*, i.e., the system's true operating mode* m_i *is guaranteed to be isolated uniquely as*

$$\mathcal{I}_{\text{FDI}}(m_i) : \hat{\mathbb{X}}_k^{(i)} \neq \emptyset,\ \left(\hat{\mathbb{X}}_k^{(0)}, \hat{\mathbb{X}}_k^{(j)}\right) = \emptyset,\ \forall \text{ pairs } (i \neq j). \tag{4.52}$$

Proof. The proof is similar to the proof of Theorem 4.3. In order to prove Theorem 4.4 we have to establish the relation between the virtually verified fault isolability condition (4.52) and condition (4.51b). To this end, we have to relate (4.52) to the substitute fault isolation condition (4.51c) initially. Let us therefore firstly consider the state-set estimate $\hat{\mathbb{X}}_k^{\star(i,j)}$ that is calculated by means of the following estimator

$$\text{ESVE}\Big(\big(\Sigma^{\star(i,j)}, \Omega_{\mathcal{E}}^{\star(i,j)}\big), \big\{u_\rho, y_\rho\big\}_0^k\Big) = \hat{\mathbb{X}}_k^{\star(i,j)} \neq \emptyset,\ \hat{\mathbb{X}}_k^{\star(i,j)} \subseteq \hat{\mathbb{X}}_k^{(i,j)} \tag{4.53}$$

utilizing the augmented state model $\Sigma^{\star(i,j)} = \Sigma \circ \big(\Delta^{\star(i)}, \Delta^{(j)}\big)$, with $\Delta^{\star(i)}$ denoting the (fictitious) exosystem describing the i-th fault exactly. Due to the exactness of $\Delta^{\star(i)}$ it holds that $\Omega_{\mathcal{E}}^{\star(i,j)} = \Omega^{(j)}$, which implies the following equivalence:

$$\mathcal{I}^\star(m_i) : \big(\xi_k^{(i)} = \xi_{\mathcal{H}}^{(i)} := 0\big) \notin \hat{\mathbb{X}}_k^{\star(i,j)},\ \big(\xi_k^{(j)} = \xi_{\mathcal{H}}^{(j)} := 0\big) \in \hat{\mathbb{X}}_k^{\star(i,j)},\ \forall \text{ pairs } (i \neq j) \ \Leftrightarrow\ \mathcal{I}_{\text{FDI}}(m_i).$$

Because $\hat{\mathbb{X}}_k^{(i,j)} \supseteq \hat{\mathbb{X}}_k^{\star(i,j)}$ for all k, we have $\mathcal{I}(m_i) \Rightarrow \mathcal{I}_{\text{FDI}}(m_i) \Leftrightarrow \mathcal{I}^\star(m_i)$. Hence, the fault-mode m_i is isolated uniquely as $\mathcal{I}_{\text{FDI}}(m_i)$ as soon as (4.51c) is satisfied. The application of Proposition 4.2 finally completes the proof. ∎

From Theorem 4.4 it follows that a robust FDI determining the set (4.42a) is guaranteed to isolate a fault uniquely, if the (i,j)-th augmented systems are observable (under the knowledge of the exogenous inputs) and, if relation (4.51b) holds for all pairs of modes. Thereby, the first condition directly relates to the property of nominal fault-isolability (see Theorem 3.2). Similar to the detection case, the required trade-off between achievable robustness and performance is indicated by condition (4.51b). Whereas the afore introduced fault-detection condition has been outlined by means of Figure 4.7, a graphical illustration of Theorem 4.4 turns out to be more complicated (due to the additional fault-state dimension) and is therefore abandoned. However both theorems bear on exactly the same principle. Hence, the outlined illustrations are also helpful for a better understanding of the above derived results on fault-isolability.

Theorem 4.3 and 4.4 link the magnitudes of the real fault-states $\xi_k^{(i)}$ to the estimated uncertainty ellipsoids $\hat{\mathbb{X}}_k^{(i)}$, $i \in \{0, \ldots, N\}$, and that way to the modeling uncertainties $\tilde{Q}_k^{(i)}$ and $\tilde{R}_k^{(i)}$. It emanates from the conditions (4.47b) and (4.51b) that a unique and robust FDI can be gained only, if the uncertainties $\tilde{Q}_k^{(i)}$ and $\tilde{R}_k^{(i)}$ are sufficiently small with respect to the minimum fault magnitudes as aimed to be diagnosed. It is also clear that the well-posedness-Assumption 4.4

can be definitely reasoned whenever the conditions (4.47b) and (4.51b) are satisfied. On the other hand, as long as $\hat{\mathbb{X}}_k^{(i)}$ and therefore $\tilde{Q}_k^{(i)}$ and $\tilde{R}_k^{(i)}$ are in due proportion to the aimed fault-sensitivity, one can argue that undetected faults have to alloy the system weakly, hence are tolerable and can be assigned to the fault-free mode.

Remark 4.13 *The existence of uniform upper bounding matrices $P_{max}^{(i)}$, $P_{max}^{(i,j)}$ (as implied by the observability of $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ and $\left(\Sigma^{(i,j)}, \Omega_{\mathcal{E}}^{(i,j)}\right)$ respectively) enables the determination of the thresholds $\theta_k^{(i)}$ and $\theta_k^{(i,j)}$ and therefore states a necessary condition for the existence of a finite fault-state $\xi_k^{(i)}$ satisfying relations* (4.47b) *and* (4.51b)*. However it may be insufficient, if the matrices $P_k^{(i)}$, $P_k^{(i,j)}$ depend on $\xi_k^{(i)}$ so that an increasing magnitude of $\xi_k^{(i)}$ causes also a magnification of $P_k^{(i)}$, $P_k^{(i,j)}$ in direction of the $\xi_k^{(i)}$-axis. This may happen, if $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ and $\left(\Sigma^{(i,j)}, \Omega_{\mathcal{E}}^{(i,j)}\right)$ are not globally observable in $\xi_k^{(i)}$ and in cases where the ESVE's linearization error scales up with the magnitude of $\xi_k^{(i)}$. In such fortunately rather uncommon special cases, uniform upper bounding matrices $P_{max}^{(i)}$, $P_{max}^{(i,j)}$ exist, however exceed the finite domains of definition of the variables $x_k^{(i)}$ and $x_k^{(i,j)}$ respectively.*

4.4 General Robust FDI Scheme (Switching Case)

In this section, a novel, more general algorithm for robust FDI is proposed that enables to compute the set of estimated modes (4.45a) also in switching diagnosis environments. Therefore, the basic FDI scheme (4.46) is extended to the switching case and mode changes are also considered during the FDI process. By this means the suggested algorithm can be utilized both on- and off-line and in addition, is capable to diagnose intermittent fault types.

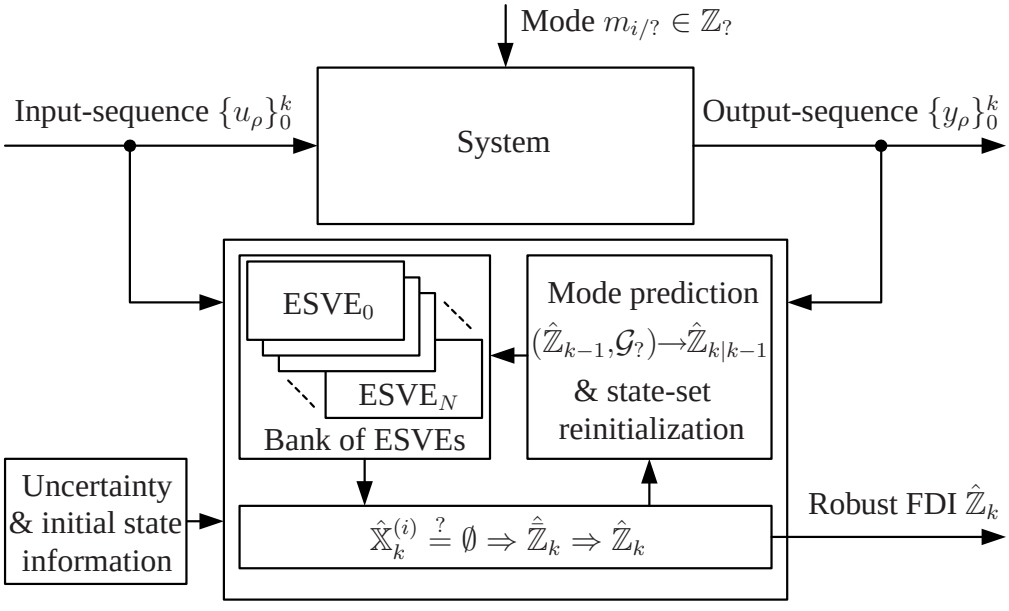


Figure 4.8: Robust FDI architecture (switching case).

The architecture of the new FDI scheme is illustrated by Figure 4.8 and basically consists of the following three components: 1) A bank of ESVEs maintaining one estimator per mode, 2) a mode-validation unit verifying the state-set estimates and determining the robust FDI $\hat{\mathbb{Z}}_k$ according to (4.45a), and 3) a generalization of the FDI function initiating and re-initializing new estimators under the terms of the underlying fault-scenario.

The computation of this scheme basically proceeds in two steps, the *prediction step* and the *correction step*. The prediction step deduces possible mode transitions under the terms of the underlying fault-scenario $\mathcal{G}_?$ and determines the predicted set of modes $\hat{\mathbb{Z}}_{k|k-1}$. In the correction step, the actual I/O-sequence $\{u_\rho, y_\rho\}_0^k$ is taken into account and is utilized for correcting the predicted mode-set as $\hat{\mathbb{Z}}_{k|k-1} \rightarrow \hat{\mathbb{Z}}_k$. Thereby, both computation steps are in brisk interaction with each other since the prediction of $\hat{\mathbb{Z}}_{k|k-1}$ not only depends on the foregoing estimated set of modes $\hat{\mathbb{Z}}_{k-1}$ but also on the result of a preceded validation of the fault-free mode. A more precise investigation of these two computation steps is outlined in the following.

Prediction step:

The prediction step deduces possible mode transitions $m_i \in \hat{\mathbb{Z}}_{k-1} \xrightarrow{\sigma_k} m_j \in \hat{\mathbb{Z}}_{k|k-1}$, $(i,j) \in \{0,\ldots,N\}$ under the terms of the underlying fault-scenario $\mathcal{G}_?$ and determines the predicted set of modes as

$$\hat{\mathbb{Z}}_{k|k-1} = \left\{ z_k \in \mathbb{Z} \,\middle|\, (z_{k-1}, \sigma_k, z_k) \in \mathcal{G}_?,\ z_{k-1} \in \hat{\mathbb{Z}}_{k-1} \right\}. \tag{4.54}$$

The derivation of (4.54) depends on the foregoing derived estimation $\hat{\mathbb{Z}}_{k-1}$ and on the following mode transition guard:

$$\sigma_k \in \left\{ \sigma_{\mathcal{H}} : \hat{\mathbb{X}}_k^{(0)} \neq \emptyset,\ \sigma_{\mathcal{F}} : \hat{\mathbb{X}}_k^{(0)} = \emptyset \right\}. \tag{4.55}$$

The guards $\sigma_{\mathcal{H}}$ and $\sigma_{\mathcal{F}}$ are events denoting healthy transitions being directed towards the fault-free mode and faulty transitions pointing to the faulty modes respectively. So it is clear from (4.54), that the computation of $\hat{\mathbb{Z}}_{k|k-1}$ requires the guards (4.55) to be verified beforehand as

$$\text{ESVE}\left(\left(\Sigma^{(0)},\ \Omega_{\mathcal{E}}^{(0)}\right), \left\{u_\rho, y_\rho\right\}_{k-\ell_0}^{k} \right) = \hat{\mathbb{X}}_k^{(0)} \stackrel{?}{=} \emptyset. \tag{4.56}$$

Hence, at any time k, the state-set estimate $\hat{\mathbb{X}}_k^{(0)}$ is computed and checked prior to the prediction of the remaining modes of $\hat{\mathbb{Z}}_{k|k-1}$.

Correction step:

Only if $\sigma_k = \sigma_{\mathcal{F}}$ holds, the predicted set of modes $\hat{\mathbb{Z}}_{k|k-1}$ contains fault-modes m_i that have to be validated by checking

$$\text{ESVE}\left(\left(\Sigma^{(i)},\ \Omega_{\mathcal{E}}^{(i)}\right), \left\{u_\rho, y_\rho\right\}_{k-\ell_i}^{k} \right) = \hat{\mathbb{X}}_k^{(i)} \stackrel{?}{=} \emptyset,\ i \in \{1,\ldots,N\}. \tag{4.57}$$

On the other hand, the computation of (4.57) is skipped, if $\sigma_k = \sigma_{\mathcal{H}}$. Applying (4.45b) and the cases of (4.45a) finally leads to the robust FDI $\hat{\mathbb{Z}}_k$, which serves as basis for the recursion of the next time step.

As in the nominal case, the key to cope with switching uncertain FDI problems is a proper *re-initialization* of the mode-conditioned state-set estimation steps. However, due to the hard reasoning of the employed mode validation principle, the hybrid estimation approach of Chapter 3 cannot be employed straight forwardly. Hence, an adequate method for re-initializing the mode-conditioned ESVE computations (4.56) and (4.57) has to be derived.

With regard to the re-initialization of the i-th mode conditioned ESVE determining the set $\hat{\mathbb{X}}_k^{(i)}$, $i \in \{0, \ldots, N\}$, there are two cases which may arise in continuing from one estimation step to the next: The ESVE is based on a predicted mode that 1) has been validated beforehand, i.e., on $\left(m_i \in \hat{\mathbb{Z}}_{k|k-1}, m_i \in \hat{\mathbb{Z}}_{k-1}\right)$ and 2) has been invalidated beforehand, i.e., $\left(m_i \in \hat{\mathbb{Z}}_{k|k-1}, m_i \notin \hat{\mathbb{Z}}_{k-1}\right)$. For both cases,

$$\hat{\mathbb{X}}_{k-\ell_i-1}^{(i)} := \begin{cases} \hat{\mathbb{X}}_{k-\ell_i-1}^{(i)} & \text{for} \quad \hat{\mathbb{X}}_{k-1}^{(i)} \neq \emptyset \\ \hat{\mathbb{X}}_{\mathcal{R}}^{(i)} & \text{for} \quad \hat{\mathbb{X}}_{k-1}^{(i)} = \emptyset \end{cases} \quad \text{with} \quad \ell_i := \begin{cases} 0 & \text{for} \quad \hat{\mathbb{X}}_{k-1}^{(i)} \neq \emptyset \\ M & \text{for} \quad \hat{\mathbb{X}}_{k-1}^{(i)} = \emptyset \end{cases} \tag{4.58}$$

gives an appropriate re-initialization scheme, where $\hat{\mathbb{X}}_{k-\ell_i-1}^{(i)}$ denotes the left fringe of the moving estimation window $[k - \ell_i - 1, \ldots, k]$. In the first case, the i-th mode-conditioned estimation window is set to length $\ell_i := 0$ and therefore $\hat{\mathbb{X}}_{k-\ell_i-1}^{(i)} := \hat{\mathbb{X}}_{k-1}^{(i)}$. Hence, the i-th mode-conditioned ESVE continues without cease. In the second case, a new ESVE is deduced starting at $\ell_i := M$ and is re-initialized as $\hat{\mathbb{X}}_{k-M-1}^{(i)} := \hat{\mathbb{X}}_{\mathcal{R}}^{(i)}$; where $\hat{\mathbb{X}}_{\mathcal{R}}^{(i)}$ is a compact not necessarily small ellipsoid satisfying $\hat{\mathbb{X}}_{\mathcal{R}}^{(i)} \supset \hat{\mathbb{X}}_k^{(i)}$ for all k.

By using the re-initialization scheme (4.58), the ESVE computations of predicted and foregoing validated modes are continued while on the other hand, the ESVEs of afore invalidated modes are brought back to the FDI procedure. Under the afore investigated fault-detectability and -isolability conditions, the choice of $M \geq \max_{(i,j)\in\{0,\ldots,N\}} n_x^{(i,j)}$ ensures the mode-conditioned estimation windows always to have a minimum length such that the estimates $\hat{\mathbb{X}}_k^{(i)}$ give meaningful results. By the choice of $\hat{\mathbb{X}}_{\mathcal{R}}^{(i)}$, it is guaranteed that none of the actual system states is excluded while re-initializing new ESVEs in the second case.

Remark 4.14 *Note that both* (4.56) *and* (4.57) *can be interpreted as kinds of moving horizon estimators since the recursively evaluated I/O-sequences* $\left\{u_\rho, y_\rho\right\}_{k-\ell_i}^{k}$, $i \in \{0, \ldots, N\}$, *determine data windows which progress with consecutive time* k. *For a more detailed discussion regarding moving horizon estimation, the interested reader is directed e.g. to (Muske and Rawlings, 1995; Muske and Edgar, 1997; Rao and Rawlings, 2000) and (Rao* et al., *2003).*

By virtue of (4.58), the evaluated moving estimation windows vary in their lengths depending on the mode transitions that are passed during the FDI process. This characteristic behavior is illustrated in Figure 4.9 by means of an exemplary two-mode intermittent fault scenario: The fault-free operation of the system between the times $k - 11$ and $k - 7$ is correctly identified by

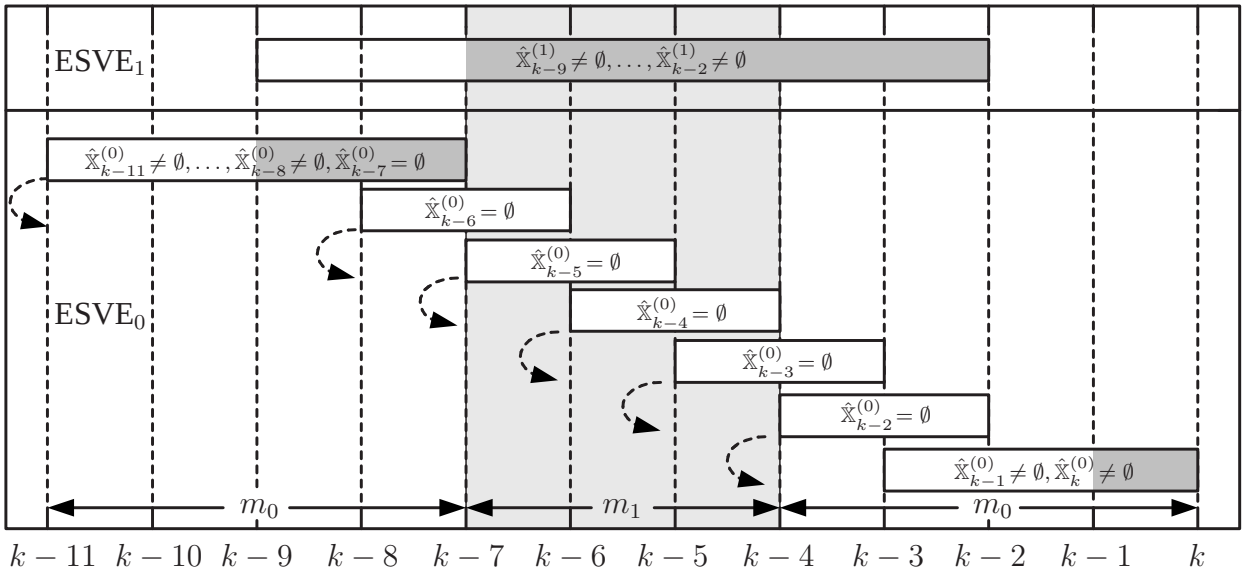


Figure 4.9: Graphical illustration of the estimation/re-initialization procedure for an exemplary two-mode fault scenario containing the modes m_0 and m_1, where $M = 3$. The intermittent fault-mode m_1 impacts the system between the times $k-7$ and $k-4$. Whereas the fault-mode m_1 is detected immediately at time $k-7$, the recovery to the fault-free operation m_0 is detected with a slight delay of three time steps at $k-1$.

the ESVE that is conditioned on the mode m_0 (ESVE$_0$). According to the first case of (4.58), the estimation window $[k-11, \ldots, k-9]$ is elongated to the time $k-7$ (illustrated by the gray area) until the mode m_1 is detected as $\hat{\mathbb{X}}^{(0)}_{k-7} = \emptyset$. The detection of the faulty mode enables the transition guard (4.55) and initiates so the deduction of a new ESVE that is conditioned on the mode m_1 (ESVE$_1$) at time $k-7$. Due to the employed moving horizon estimation principle, the ESVE$_1$ goes back to time $k-9$ and is re-initialized as $\hat{\mathbb{X}}^{(1)}_{k-9} := \hat{\mathbb{X}}^{(1)}_{\mathcal{R}}$. The estimation horizon $[k-9, \ldots, k-7]$ is elongated to the time $k-2$ until at time $k-1$, the mode m_0 is determined to be valid again as $\hat{\mathbb{X}}^{(0)}_{k-1} \neq \emptyset$. In order to check whether the system operates still faulty or again fault-free, new ESVE$_0$ estimators are deduced and evaluated at any time between $k-6$ and $k-2$. Thereby, each of the estimators is re-initialized as $\{\hat{\mathbb{X}}^{(0)}_{k-6}, \ldots, \hat{\mathbb{X}}^{(0)}_{k-2}\} := \hat{\mathbb{X}}^{(0)}_{\mathcal{R}}$. By this, the system is diagnosed to operate again fault-free once the estimation window is outside the period of the faulty operation; which inherently introduces a delay of duration M in recognizing the recovery to the fault-free mode m_0.

Let us finally conclude this section by summarizing the derived results in form of the following FDI algorithm.

Algorithm 4.3 (Robust FDI of switching problems) *Suppose the uncertain structured augmented state model $\mathcal{S}_{\mathcal{U}}$ (see Definition 4.1,* (4.9)*) and the sufficiently long I/O-sequence $\{u_\rho, y_\rho\}_0^k$, $k > M = \max_{(i,j)}(n_x^{(i,j)})$, to be given. Compute the robust FDI algorithm*

$$\text{rFDI}\left(\mathcal{S}_{\mathcal{U}}, \{u_\rho, y_\rho\}_0^k\right) = \hat{\mathbb{Z}}_k. \tag{4.59}$$

Thereby, the operator rFDI$(\cdot)$ *comprises the following computation steps that are carried out at any time* k*:*

1. *Re-initialize the ESVE* (4.56) *according to* (4.58) *and determine the mode transition guard* (4.55)*.*
2. *Compute the set of predicted modes* $\hat{\mathbb{Z}}_{k|k-1}$ *under the terms of the underlying fault-scenario and the mode transition guard according to* (4.54)*.*
3. *Re-initialize the ESVEs* (4.57) *that are conditioned on the predicted fault-modes* $m_i \in \hat{\mathbb{Z}}_{k|k-1}$*,* $i \in \{1, \ldots, N\}$ *according to* (4.58)*, determine the set of estimated modes* $\hat{\mathbb{Z}}_k$ *as described in* (4.45a) *and enter the next recursion in the first computation step of the algorithm.*

Algorithm 4.3 enables to compute a robust FDI for switching and non-switching FDI problems. The following section illustrates the application of this algorithm by means of the DC actuator example.

4.5 Example - Robust FDI of the DC Actuator System

Let us illustrate the proposed robust FDI method by means of the complete and uncertain configuration of the DC actuator example as originally introduced in Section 2.3. Thereby, the nonlinear problem configuration is considered including additionally continuous modeling uncertainties of the system and the exosystem models.

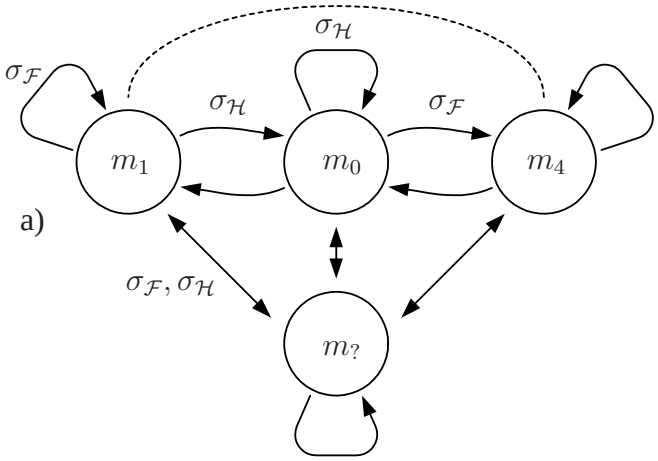
4.5.1 Fault Representation, Fault Scenario, and Uncertain Structured Augmented State Model

The DC actuator is described by the uncertain model (2.12) with uncertainty bounds (2.13-2.14) and is considered subject to the four fault-candidates $\mathcal{F}_1, \ldots, \mathcal{F}_4$. Each of the faults is described by an uncertain constant-type exosystem of the form

$$\Delta_i : \begin{cases} \xi_{k+1}^{(i)} = \xi_k^{(i)} + \lambda_k^{(i)},\ k \geq 0,\ \xi_0^{(i)} \\ \xi_{\mathcal{H}}^{(i)} = 0 \\ \delta_k^{(i)} = \xi_k^{(i)} \\ \delta_{\mathcal{H}}^{(i)} = 0 \end{cases} , \ i \in \{1, \ldots, 4\}. \tag{4.60}$$

Thereby, the unknown-but-bounded uncertainties $\lambda_k^{(i)}$ are constrained to the following compact sets

$$\mathbb{L}^{(1,\ldots,4)} : \left\{ |\lambda_k^{(1)}| \leq \bar{\lambda}^{(1)} = 0.6, |\lambda_k^{(2)}| \leq \bar{\lambda}^{(2)} = 0.6, |\lambda_k^{(3)}| \leq \bar{\lambda}^{(3)} = 6.0, |\lambda_k^{(4)}| \leq \bar{\lambda}^{(4)} = 0.15 \right\} \tag{4.61}$$



b)

z_{k+1}	z_k	σ_k
m_0	m_0	$\sigma_{\mathcal{H}}$
m_1	m_0	$\sigma_{\mathcal{F}}$
$\vdots$	$\vdots$	$\vdots$
m_4	m_0	$\sigma_{\mathcal{F}}$
$m_?$	m_0	$\sigma_{\mathcal{F}}$
m_0	m_1	$\sigma_{\mathcal{H}}$
m_1	m_1	$\sigma_{\mathcal{F}}$
$m_?$	m_1	$\sigma_{\mathcal{F}}$
$\vdots$	$\vdots$	$\vdots$
m_0	m_4	$\sigma_{\mathcal{H}}$
m_4	m_4	$\sigma_{\mathcal{F}}$
$m_?$	m_1	$\sigma_{\mathcal{F}}$
$m_?$	$m_?$	$\sigma_{\mathcal{F}}$
m_0	$m_?$	$\sigma_{\mathcal{H}}$
$\vdots$	$\vdots$	$\vdots$
m_4	$m_?$	$\sigma_{\mathcal{H}}$

Figure 4.10: a) Mode transition graph and b) automaton table of the uncertain state automaton that models the underlying single-fault scenario. This captures the fault-free case m_0, the four anticipated single-faults $\mathcal{F}_1, \ldots, \mathcal{F}_4$ (modes $m_1, \ldots, m_4$), and the unknown mode $m_?$.

and the exosystem initial state uncertainties to

$$\Xi^{(1,\ldots,4)} : \left\{ |\xi_0^{(1)}| \leq 5,\ |\xi_0^{(2)}| \leq 2,\ |\xi_0^{(3)}| \leq 20,\ |\xi_0^{(4)}| \leq 0.45 \right\}. \tag{4.62}$$

The exosystem uncertainties (4.61) and (4.62) are directly added to the fault inputs $\delta_k^{(i)}$ that enter the DC actuator system. Hence they have the same physical units and their magnitudes are chosen in an adequate relation to the expected fault magnitudes as impressed in the subsequently performed simulations.

The mode-conditioned uncertain augmented state models $\left(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\right)$ are obtained in the manner already described in Section 3.5.2, whereas the augmented uncertainty inputs lump the uncertainties (4.61) and the plant-model-mismatch (2.13-2.14). Using the results of Section 4.2.2.2, the outer ellipsoidal uncertainty bounds $\Omega_{\mathcal{E}}^{(i)}$ are given as

$$\Omega_{\mathcal{E}}^{(i)} : \left\{ x_0^{(i)} \in \mathcal{E}\left(0, P_0^{(i)}\right),\ w_k^{(i)} \in \mathcal{E}\left(0, Q^{(i)}\right),\ v_k^{(i)} \in \mathcal{E}\left(0, R^{(i)}\right),\ \forall\, k, \right. \tag{4.63}$$

where $P_0^{(1)} = \frac{1}{3}\,\mathrm{diag}\left([8\ 1000\ 5]^T\right)^{-2}, \ldots, P_0^{(4)}$, $Q^{(1)} = \frac{1}{3}\,\mathrm{diag}\left([0.1\ 2.0\ 0.6]^T\right)^{-2}, \ldots, Q^{(4)}$, and $R^{(1)}, \ldots, R^{(4)} = \frac{1}{2}\,\mathrm{diag}\left([0.01\ 0.02]^T\right)^{-2}$.

By this means, the uncertain structured augmented state model of the DC actuator is given as follows:

$$\mathcal{S}_{\mathcal{U}} := \Big\{ \big(\Sigma^{(i)}, \Omega_{\mathcal{E}}^{(i)}\big), i \in \{0, \ldots, 4\}, \big(\Sigma^{(?)}, \Omega^{(?)}\big), \mathcal{A}_? \Big\}. \tag{4.64}$$

The tuple $\mathcal{S}_{\mathcal{U}}$ contains the mode-specific continuous models and the discrete-state automaton $\mathcal{A}_?(\cdot)$ defining the rule-type of the assumed single-fault scenario. Among the anticipated operating modes $m_1, \ldots, m_4$, the automaton $\mathcal{A}_?(\cdot)$ incorporates the unknown mode of operation $m_?$. The topology of the employed state automaton is illustrated in Figure 4.10 and is formally defined/implemented by the contained automaton table.

4.5.2 Numerical Results

The numerical simulation is performed by evaluating the test-scenario of Table 3.1 using MATLAB/SIMULINK. The robust FDI is computed according to Algorithm 4.3 as

$$\text{rFDI}\Big(\mathcal{S}_{\mathcal{U}}, \big\{u_\rho, y_\rho\big\}_0^k\Big) = \hat{\mathbb{Z}}_k, \tag{4.65}$$

where a moving estimation window of length $M = 4$ is employed. The approach used to bound the ESVE linearization errors is to use the free interval mathematics toolbox provided by Zemke[2].

In Figure 4.11 a), the gradually increasing magnitudes of the intermittently impacting faults are shown. Figure 4.11 b) illustrates the chronology of the estimated set of modes. This scales down incrementally until the faults are uniquely detected and isolated at the time the corresponding fault magnitudes exceed their specific detection and isolation thresholds. Also the faulty modes' recoveries are recognized immediately. According to the employed switching FDI scheme, the number of ESVE computations is variant in time (see Figure 4.11 c)) and depends on the based single-fault scenario.

The results outlined in Figure 4.12 are obtained in a similar way, however, are based on a worse model assuming an increased continuous model uncertainty of 150%. Accordingly, the individual modes are detected/isolated with a larger delay. This is reasoned in that the imposed fault magnitudes have to increase further in order to exceed the enlarged thresholds resulting from the enhanced uncertainty bounds. Due to the enlarged uncertainty, the fault-modes m_1 and m_2 cannot be distinguished anymore, however, are not excluded from the estimated set of modes. Hence, the computed FDI is robust but non-unique.

Figure 4.13 considers again the 100% uncertainty case, whereas the faults impact the system abruptly. To that effect, the faults are detected and isolated without delay since the fault-specific detection/isolation thresholds are exceeded immediately. Thereby, the system is diagnosed for a

[2]The free Interval Arithmetic Toolbox for MATLAB provided by J. Zemke is online available at: `http://www.ti3.tu-harburg.de/~zemke/b4m/index.html`.

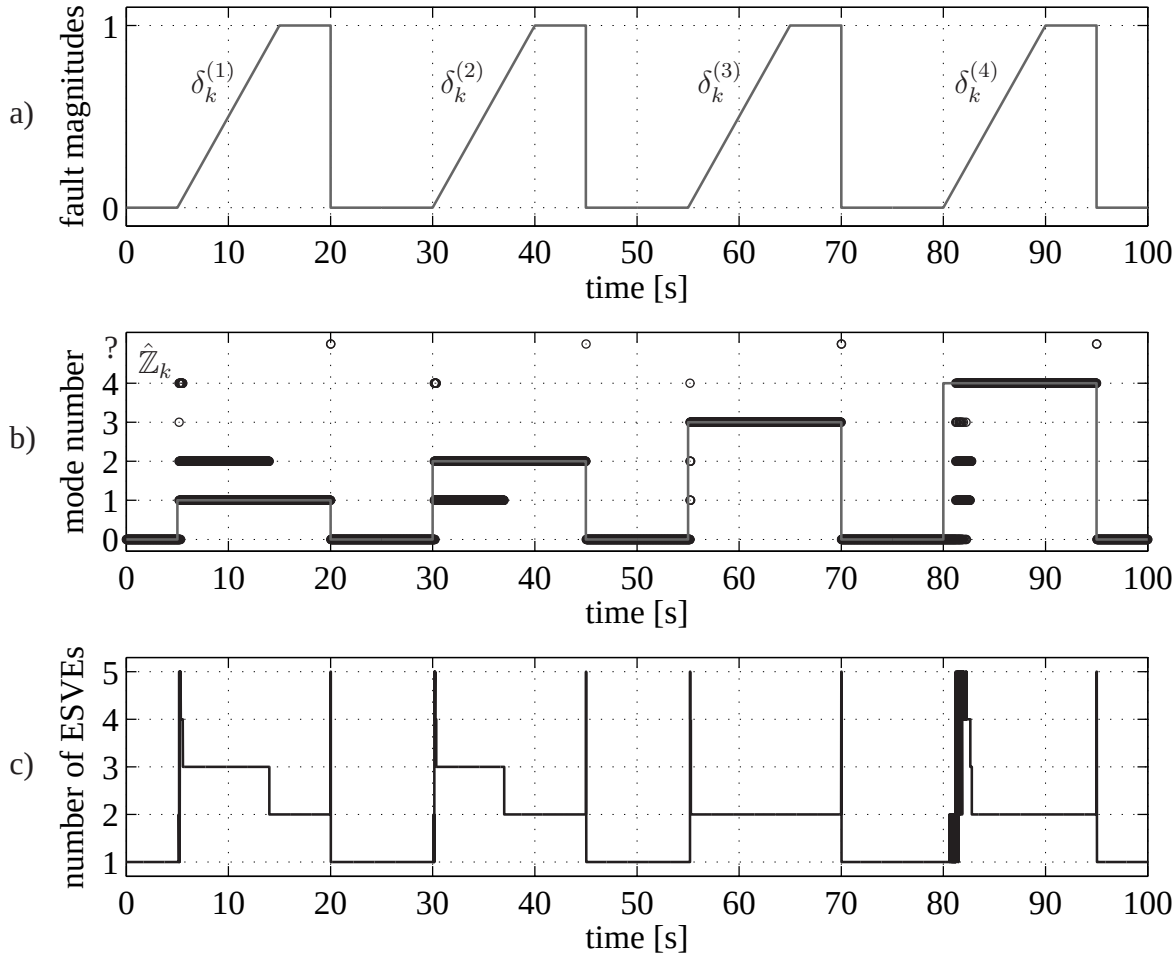


Figure 4.11: Robust FDI of the DC actuator system (incipient faults). a) Imposed (normalized) fault magnitudes. b) Imposed (solid) and estimated (circled) mode sequences. c) Number of simultaneously computed ESVEs.

while to operate in the unknown mode whenever there is a jump in the fault magnitudes (see also in the Figures 4.11 and 4.12 when the system recovers step-wise the fault-free mode). This is due to the fact that the uncertainty bounds of the employed exosystems are temporarily exceeded by the

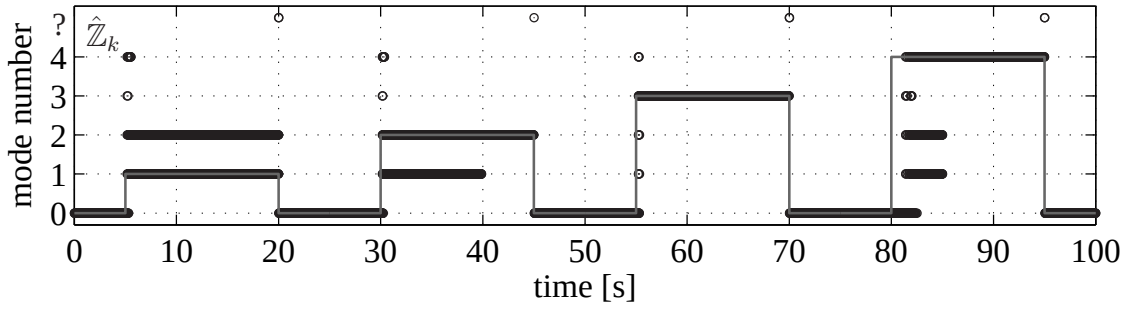


Figure 4.12: Robust FDI of the DC actuator system (incipient faults) with 150 % continuous model uncertainty: Imposed (solid) and estimated (circled) mode sequences for the fault magnitudes outlined in Figure 4.11 a).

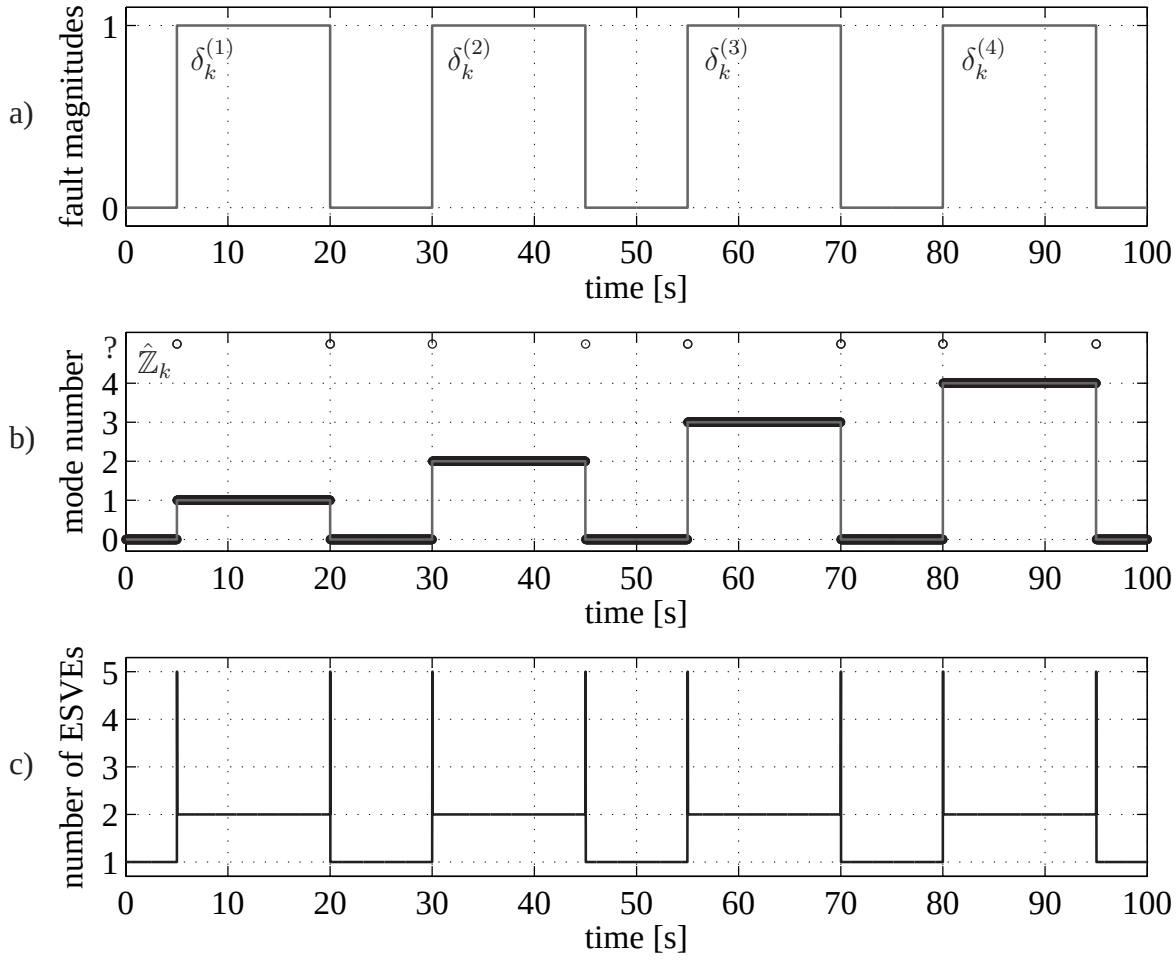


Figure 4.13: Robust FDI of the DC actuator system (abrupt faults). a) Imposed (normalized) fault magnitudes. b) Imposed (solid) and estimated (circled) mode sequences. c) Number of performed ESVE computations.

jumping fault magnitudes for a short period of time. Of course, these unknown mode transitions could be avoided by enlarging the fault-specific uncertainty bounds, however at the expense of the attainable fault-sensitivity. Hence, the concept of the unknown mode may be also helpful in order to avoid excessively conservative uncertainty formulations.

By means of the DC actuator example, the suggested robust FDI method is illustrated. It is shown to be capable for tackling a variety of challenging situations that may appear in FDI applications considering such systems. Both incipient and abrupt faults are considered and shown to be correctly detected/isolated despite of the model uncertainties, even in a switching diagnosis environment. Unforeseen large model uncertainties that are not captured by the model are immediately recognized and correctly assigned to the unknown mode of operation. At any time, the system's true operating mode is contained within the estimated set of modes - which verifies the robustness of the provided FDI algorithm. The number of ESVEs that are computed at any time varies depending on the topology of the underlying state automaton and underruns the total number of modes significantly at most times. In off-line FDI applications, which often require an iterative

evaluation of long measurement sequences, this may help to drastically reduce computational effort. Two uncertainty settings assuming differently large uncertainty bounds are considered and analyzed with respect to their influence on the fault detection and isolation behavior. Increasing uncertainty bounds are shown to complicate the performed process of elimination as certain modes become (temporarily) indistinguishable. This observed behavior does not prove a weakness of the suggested FDI approach. In fact it confirms our robust fault detectability and isolability conditions stating that desired robustness and fault sensitivity have to be well-balanced in order to allow for a unique FDI.

4.6 Summary

The results of the pervious chapter are the basis to extend the structured augmented state modeling formalism to uncertain nonlinear systems. Similar to the nominal case, the overall model for describing the uncertain problem is a hybrid state automaton. With respect to the nominal representation, this basically differs in the additionally incorporated unknown-but-bounded uncertainty inputs as well as in the modified topology of the discrete-state automaton including the unknown mode of operation.

The key to the robust FDI with uncertain structured augmented state models is also augmented state estimation. However, due to the employed unknown-but-bounded uncertainty representation, the augmented state estimation problem turns out to be set-valued: Instead of determining point-estimates of the system's true augmented state, estimated sets of states are computed that are guaranteed to contain the true state. By means of the i-th mode-conditioned uncertain augmented state model, the ideal but computationally intractable solution to nonlinear set-valued augmented state estimation (NSVE) is outlined. In reference to the ideal approach, the approximate extended set-valued augmented state estimation scheme (ESVE) is motivated and extensively reviewed. An application oriented summary of the ESVE algorithm's implementation and its most important properties is brought together from different papers, which is also valuable for engineers working in the field of robust state estimation.

Fundamental relations between NSVE/ESVE and robust FDI are established whereas the link between these two otherwise different fields is basically given by mode-conditioned uncertain model-validation. The robust FDI problem is defined and the ideal but computationally intractable solution based on the ideal NSVE algorithm is derived. A computationally tractable alternative utilizing the ESVE algorithm is suggested and proven to determine a robust FDI. Robust fault-detection and -isolation conditions are introduced stating that, provided the underlying FDI problem satisfies a certain well-posedness assumption, the gained robust FDI is meaningful, i.e., is unique. Uncertainty-dependent detection and isolation thresholds on the true fault magnitudes are derived

which have to be exceeded in order that these faults can be guaranteed to be detected/isolated by the proposed FDI scheme. Both conditions disclose the inherent tradeoff between attainable fault sensitivity and robustness.

A generally applicable robust FDI scheme is provided that allows to diagnose non-switching and switching FDI problems. Besides off-line FDI tasks and the diagnosis of persistent fault-types, this scheme can be used on-line and for coping with intermittent fault types. The core of this robust FDI algorithm forms a novel moving horizon based re-initialization scheme. This initiates and re-initializes the mode-conditioned ESVEs according to the rule-type of the assumed fault-scenario and furthermore guarantees the evaluated estimation windows to be sufficiently large in order that meaningful results are obtained. The resulting FDI is robust in that the estimated set of modes is guaranteed and unanticipated faults are isolated as an unknown mode of operation.

The suggested concept is illustrated for the robust FDI of the DC actuator example. Although the model of the DC actuator is uncertain, the systematic incorporation of the uncertainty bounds within the robust FDI design maintains the desired fault detection and isolation capability. Thereby, a remarkable feature of the proposed method is that the robust FDI design is performed in a straightforward manner. The simulation results approve the properties of the suggested diagnosis algorithm and the conclusion of the fault-detectability and -isolability conditions.

Chapter 5

Application to the Three-Tank Benchmark

This application chapter presents the robust fault diagnosis of the three-tank system by using the afore introduced method of robust FDI. The three-tank system is a popular benchmark problem for model-based FDI. It is therefore well-suited to test our robust FDI method and to compare the results with alternative approaches.

Various FDI concepts have been proposed in the FDI literature for diagnosing the three-tank benchmark, e.g., linear FDI by parity relations (Isermann, 1997), nonlinear FDI by differential-algebraic approaches (Join *et al.*, 2005), or robust nonlinear FDI by using neural networks (Zhang *et al.*, 2002). A comparison between the linear observer-based approach, the parameter estimation approach, and the neural network based approach to the tree-tank FDI can be found in (Köppen-Seliger *et al.*, 1999). The most distinguishing features of these approaches are given by their linear/nonlinear systems capability and their ability to cope with modeling uncertainties and different kinds of fault-types.

In the following, our previously introduced robust FDI method is employed for the diagnosis of the three-tank benchmark. This is considered to operate subject to input-, system-, and output-type faults occurring both incipiently and abruptly. Thereby, the involved model of the three-tank is uncertain and the measurements are corrupted by noise. Beyond these continuous modeling uncertainties, an exemplary unknown mode situation is examined considering the three-tank diagnosis under the influence of an unanticipated multiple-fault. It will be exemplified that the provided diagnosis scheme is capable to determine a nonlinear system FDI which is robust, not only against continuous modeling uncertainties but also against discrete uncertainties like unanticipated faults. The examinations of this chapter are based in part on (Aßfalg and Allgöwer, 2007).

5.1 Model of the Three-Tank

The three-tank system shown in Figure 5.1 basically consists of the three tanks, T_1, T_2, and T_3 that are identical and cylindrical in shape with a cross section A. The cross section of the pipes connecting the tanks is S and the liquid levels in the three tanks are denoted by $x_{1,k}$, $x_{2,k}$, and $x_{3,k}$ (in [m]) respectively. The incoming flow rates that are supplied by the pumps 1 and 2 are denoted by $u_{1,k}$ and $u_{2,k}$ (in [m^3/s]) respectively.

By using balance equations and Torricelli's rule, the nonlinear discrete-time dynamics of the three-tank is obtained as

$$\Sigma : \begin{cases} u'_{1,k} = u_{1,k} + \delta_k^{(1)} \\ u'_{2,k} = u_{2,k} + \delta_k^{(5)} \\ x_{1,k+1} = x_{1,k} + \dfrac{dT}{A}\big(u'_{1,k} - q_1(x_{1,k}, x_{2,k})\big) \\ x_{2,k+1} = x_{2,k} + \dfrac{dT}{A}\big(q_1(x_{1,k}, x_{2,k}) - q_2(x_{2,k}, x_{3,k}) - \delta_k^{(4)}\big) \\ x_{3,k+1} = x_{3,k} + \dfrac{dT}{A}\big(u'_{2,k} + q_2(x_{2,k}, x_{3,k}) - q_3(x_{3,k})\big) \\ y_{1,k} = x_{1,k} + \delta_k^{(2)} + v_{1,k} \\ y_{2,k} = x_{2,k} + \delta_k^{(3)} + v_{2,k} \\ y_{3,k} = x_{3,k} + \delta_k^{(6)} + v_{3,k} \end{cases}, \; x_0 = \begin{bmatrix} x_{1,0} \\ x_{2,0} \\ x_{3,0} \end{bmatrix}, \tag{5.1}$$

where $x_k = [x_{1,k}\ x_{2,k}\ x_{3,k}]^T$ is the state vector, $u_k = [u_{1,k}\ u_{2,k}]^T$ is the input vector, and $y_k = [y_{1,k}\ y_{2,k}\ y_{3,k}]^T$ is the vector of measurements taken with a sampling rate dT. The exogenous inputs $\delta_k = [\delta_k^{(1)}, \ldots, \delta_k^{(6)}]^T$, $w_k = [w_{1,k}\ w_{2,k}\ w_{3,k}]^T$ and $v_k = [v_{1,k}\ v_{2,k}]^T$ lump the effects of potential

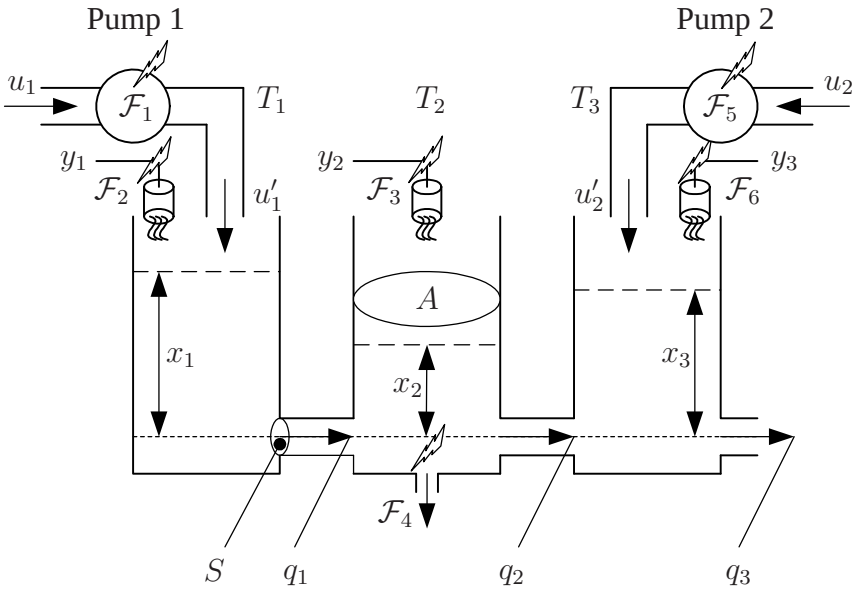


Figure 5.1: The three-tank benchmark.

Table 5.1: Model parameter values of the three-tank.

Description	Symbol	Value	Unit
Cross section of the three tanks T_1, T_2, and T_3	A	$4.0 \cdot 10^{-2}$	$[\mathrm{m}^2]$
Cross section of the connecting pipes	S	$1.6 \cdot 10^{-4}$	$[\mathrm{m}^2]$
Outflow coefficient	c	0.5	$[\cdot]$
Gravity acceleration	g	9.81	$[\mathrm{m/s}^2]$
Sampling rate	dT	1.0	[s]

faults, parameter uncertainties of the cross sections S, and measurement noise respectively. The flow-rates q_1 and q_2 between the tanks and the outflow-rate q_3 are given as

$$\begin{aligned} q_1 &= c\,(S + w_{1,k})\,\mathrm{sign}(x_{1,k} - x_{2,k})\sqrt{2g|x_{1,k} - x_{2,k}|} \\ q_2 &= c\,(S + w_{2,k})\,\mathrm{sign}(x_{2,k} - x_{3,k})\sqrt{2g|x_{2,k} - x_{3,k}|}\,\cdot \\ q_3 &= c\,(S + w_{3,k})\sqrt{2g x_{3,k}} \end{aligned} \tag{5.2}$$

Thereby, c denotes a nondimensional outflow coefficient and g is the gravity acceleration. The initial state of the three-tank is $x_0 = [0.36\ 0.32\ 0.20]^T$ (in [m]) and the steady-state flow rates supplied by the pumps 1 and 2 are chosen as $u_1 = 1.0 \cdot 10^{-4}$ and $u_2 = 7.0 \cdot 10^{-5}$ (in $[\mathrm{m}^3/\mathrm{s}]$). The nominal values of the model parameters are summarized in Table 5.1.

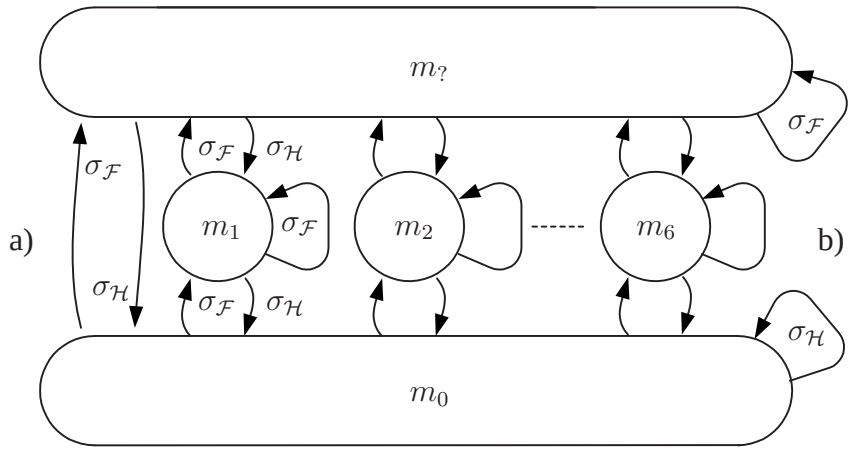
5.1.1 Fault Representation, Fault Scenario, and Unknown Mode

The three-tank system is considered subject to six candidates for potential faults $\mathcal{F}_1, \ldots, \mathcal{F}_6$, which may appear both incipiently and abruptly. The anticipated faults (that are also illustrated in Figure 5.1) can be described as follows:

1. *Input-faults $\mathcal{F}_1$ and $\mathcal{F}_5$ (actuator faults in pumps 1 and 2).* Two additive actuator faults $\mathcal{F}_1$ and $\mathcal{F}_5$ in pumps 1 and 2 respectively are considered. Due to the input-faults, the incoming supply flow rates $u'_{1,k} = u_{1,k} + \delta_k^{(1)}$ and $u'_{2,k} = u_{2,k} + \delta_k^{(5)}$ deviate by $\delta_k^{(1)}$ and $\delta_k^{(5)}$ from the desired input values $u_{1,k}$ and $u_{2,k}$ respectively.

2. *Output-faults $\mathcal{F}_2$, $\mathcal{F}_3$, and $\mathcal{F}_6$ (defective liquid level sensors in tanks 1, 2, and 3).* Three additive sensor faults in tanks 1, 2 and 3 are considered. Due to the sensor-faults $\mathcal{F}_2$, $\mathcal{F}_3$, and $\mathcal{F}_6$, the measured values of the liquid levels $y_{1,k} = x_{1,k} + \delta_k^{(2)}$, $y_{2,k} = x_{2,k} + \delta_k^{(3)}$, and $y_{3,k} = x_{3,k} + \delta_k^{(6)}$ deviate by $\delta_k^{(2)}$, $\delta_k^{(3)}$, and $\delta_k^{(6)}$ from the real liquid levels $x_{1,k}$, $x_{2,k}$, and $x_{3,k}$ respectively.

3. *System-fault $\mathcal{F}_4$ (leakage in tank 2).* One system-fault affecting the second tank is considered. It is assumed that the leak is circular in shape with unknown effective area $\xi_k^{(4)}$. If



z_{k+1}	z_k	σ_k
m_0	m_0	$\sigma_\mathcal{H}$
m_1	m_0	$\sigma_\mathcal{F}$
$\vdots$	$\vdots$	$\vdots$
m_6	m_0	$\sigma_\mathcal{F}$
$m_?$	m_0	$\sigma_\mathcal{F}$
m_0	m_1	$\sigma_\mathcal{H}$
m_1	m_1	$\sigma_\mathcal{F}$
$m_?$	m_1	$\sigma_\mathcal{F}$
$\vdots$	$\vdots$	$\vdots$
m_0	m_6	$\sigma_\mathcal{H}$
m_6	m_6	$\sigma_\mathcal{F}$
$m_?$	m_1	$\sigma_\mathcal{F}$
$m_?$	$m_?$	$\sigma_\mathcal{F}$
m_0	$m_?$	$\sigma_\mathcal{H}$
$\vdots$	$\vdots$	$\vdots$
m_6	$m_?$	$\sigma_\mathcal{H}$

Figure 5.2: a) Mode transition graph and b) automaton table of the uncertain state automaton that models the underlying single-fault scenario; capturing the fault-free case m_0, the six anticipated single-faults $\mathcal{F}_1, \ldots, \mathcal{F}_6$ (modes $m_1, \ldots, m_6$), and the unknown mode $m_?$.

$\delta_k^{(4)}$ denotes the outflow rate being due to the leak, this is given by the nonlinear function $\delta_k^{(4)} = \xi_k^{(4)}\sqrt{2gx_{2,k}}$.

In the following, each of the anticipated faults $\mathcal{F}_1, \ldots, \mathcal{F}_6$ is represented by a simple constant-type exosystem, i.e.,

$$\Delta^{(\alpha)} : \begin{cases} \xi_{k+1}^{(\alpha)} = \xi_k^{(\alpha)} + \lambda_k^{(\alpha)},\ \xi_0^{(\alpha)} \\ \delta_k^{(\alpha)} = \xi_k^{(\alpha)} \\ \delta_\mathcal{H}^{(\alpha)} = 0 \end{cases}, \alpha = 1,2,3,5,6\ ,\ \Delta^{(4)} : \begin{cases} \xi_{k+1}^{(4)} = \xi_k^{(4)} + \lambda_k^{(4)},\ \xi_0^{(4)} \\ \delta_k^{(4)} = \xi_k^{(4)}\sqrt{2gx_{2,k}} \\ \delta_\mathcal{H}^{(4)} = 0 \end{cases}, \tag{5.3}$$

where each of the exosystems $\Delta^{(1)}, \ldots, \Delta^{(6)}$ is tainted with an unknown but bounded modeling uncertainty represented by $\lambda^{(1)}, \ldots, \lambda^{(6)}$. Depending on the choice of the uncertainty bounds $\bar{\lambda}^{(1)}, \ldots, \bar{\lambda}^{(6)}$, the exosystem models (5.3) can be utilized for representing both abrupt and incipient fault-types.

The mode set $\mathbb{Z}_? = \{m_0, m_1, \ldots, m_6, m_?\}$ is given by the anticipated faults $\mathcal{F}_1, \ldots, \mathcal{F}_6$, the fault-free case, and the unknown mode. Supposing a classical single-fault scenario, mode transitions

are assumed to follow the rule type of the uncertain transition relation $\mathcal{G}_?$, which is specified by the automaton table 5.2 b). The uncertain mode transition relation $\mathcal{G}_?$ contains the unknown mode $m_?$ that captures unanticipated operating modes being either due to unanticipated faults or invalid modeling uncertainties. An illustration of the employed state automaton is given by the eight-mode transition graph shown in Figure 5.2 a). By this means, the single-fault scenario is completely described by the uncertain state automaton

$$\mathcal{A}_?(\mathbb{Z}_?, \mathcal{G}_? : \mathbb{Z}_? \xrightarrow{\sigma_k} \mathbb{Z}_?, z_0), z_k \in \mathbb{Z}_?,\ \sigma_k \in \{\sigma_\mathcal{F}, \sigma_\mathcal{H}\}, \tag{5.4}$$

where z_k is a discrete-state variable which, in this example, is initialized as $z_0 = m_0$; meaning that the system operates fault-free at time $k = 0$.

5.1.2 Modeling Uncertainty and Noise Representation

The initial state uncertainties, the model uncertainties, and the measurement noise are given by the uniform uncertainty sets

$$\hat{\mathbb{X}}_0 = \begin{cases} |x_{1,0}| \leq \bar{x}_{1,0} = 0.2\,[\mathrm{m}] \\ |x_{2,0}| \leq \bar{x}_{2,0} = 0.2\,[\mathrm{m}] \\ |x_{3,0}| \leq \bar{x}_{3,0} = 0.2\,[\mathrm{m}] \end{cases}, \quad \mathbb{W} = \begin{cases} |w_{1,k}| \leq \bar{w}_1 = 0.05\,[\mathrm{m}] \\ |w_{2,k}| \leq \bar{w}_2 = 0.05\,[\mathrm{m}] \\ |w_{3,k}| \leq \bar{w}_3 = 0.05\,[\mathrm{m}] \end{cases}, \ \forall\, k \tag{5.5}$$

and

$$\mathbb{V} = \begin{cases} |v_{1,k}| \leq \bar{v}_1 = 10^{-3}\,[\mathrm{m}] \\ |v_{2,k}| \leq \bar{v}_2 = 10^{-3}\,[\mathrm{m}] \\ |v_{3,k}| \leq \bar{v}_3 = 10^{-3}\,[\mathrm{m}] \end{cases}, \ \forall\, k \tag{5.6}$$

respectively. The initial state and the model uncertainties of the fault-specific exosystem models $\Delta^{(1)}, \ldots, \Delta^{(6)}$ are bounded for all times k by the following constraints

$$\Xi^{(1,\ldots,6)} = \begin{cases} |\xi_0^{(1,5)}| \leq \bar{\xi}_0^{(1,5)} = 0.1\,[\mathrm{m}^3/s] \\ |\xi_0^{(2,3,6)}| \leq \bar{\xi}_0^{(2,3,6)} = 0.1\,[\mathrm{m}] \\ |\xi_0^{(4)}| \leq \bar{\xi}_0^{(4)} = 0.1\,[\mathrm{m}^3/s] \end{cases}, \mathbb{L}^{(1,\ldots,6)} = \begin{cases} |\lambda_k^{(1,5)}| \leq \bar{\lambda}^{(1,5)} = 10^{-5}\,[\mathrm{m}^3/s] \\ |\lambda_k^{(2,3,6)}| \leq \bar{\lambda}^{(2,3,6)} = 10^{-2}\,[\mathrm{m}] \\ |\lambda_k^{(4)}| \leq \bar{\lambda}^{(4)} = 10^{-4}\,[\mathrm{m}^3/s] \end{cases}. \tag{5.7}$$

5.1.3 Uncertain Structured Augmented State Model of the Three-Tank

The uncertain structured augmented state model is given by the tuple

$$\mathcal{S}_\mathcal{U} := \left(\left\{ \left(\Sigma^{(i)}, \Omega^{(i)}\right), i \in \{0, \ldots, 6\}, \left(\Sigma^{(?)}, \Omega^{(?)}\right) \right\}, \mathcal{A}_? \right) \tag{5.8}$$

including the above specified uncertain state automaton $\mathcal{A}_?$, the empty sets of equations $\Sigma^{(?)} = \{\cdot\}$ and $\Omega^{(?)} = \{\cdot\}$ characterizing the unknown mode, and the uncertain augmented state models

$\big(\Sigma^{(i)}, \Omega^{(i)}\big)$, $i \in [0, \ldots, 6]$. Concatenating the model of the three-tank with the fault-specific exosystem models and setting the mismatched fault characteristics to their fault-free values, i.e., $\delta_k^{(i)} := \delta_{\mathcal{H}}^{(i)} = 0$, leads to seven (augmented) state models describing the fault-free and the faulty operations of the three-tank as follows:

$$\Sigma^{(0)} \; : \; \begin{cases} u'_{1,k} = u_{1,k} \\ u'_{2,k} = u_{2,k} \\ x^{(0)}_{1,k+1} = x^{(0)}_{1,k} + \dfrac{dT}{A}\big(u'_{1,k} - q_1(x^{(0)}_{1,k}, x^{(0)}_{2,k})\big) + w^{(0)}_{1,k} \\ x^{(0)}_{2,k+1} = x^{(0)}_{2,k} + \dfrac{dT}{A}\big(q_1(x^{(0)}_{1,k}, x^{(0)}_{2,k}) - q_2(x^{(0)}_{2,k}, x^{(0)}_{3,k})\big) + w^{(0)}_{2,k} \\ x^{(0)}_{3,k+1} = x^{(0)}_{3,k} + \dfrac{dT}{A}\big(u'_{2,k} - q_2(x^{(0)}_{2,k}, x^{(0)}_{3,k}) - q_3(x^{(0)}_{3,k})\big) + w^{(0)}_{3,k} \\ y_{1,k} = x^{(0)}_{1,k} + v_{1,k} \\ y_{2,k} = x^{(0)}_{2,k} + v_{2,k} \\ y_{3,k} = x^{(0)}_{3,k} + v_{3,k} \end{cases}, \; x_0^{(0)} = \begin{bmatrix} x^{(0)}_{1,0} \\ x^{(0)}_{2,0} \\ x^{(0)}_{3,0} \end{bmatrix}$$

$$\vdots$$

$$\Sigma^{(6)} \; : \; \begin{cases} u'_{1,k} = u_{1,k} \\ u'_{2,k} = u_{2,k} \\ x^{(6)}_{1,k+1} = x^{(6)}_{1,k} + \dfrac{dT}{A}\big(u'_{1,k} - q_1(x^{(6)}_{1,k}, x^{(6)}_{2,k})\big) + w^{(6)}_{1,k} \\ x^{(6)}_{2,k+1} = x^{(6)}_{2,k} + \dfrac{dT}{A}\big(q_1(x^{(6)}_{1,k}, x^{(6)}_{2,k}) - q_2(x^{(6)}_{2,k}, x^{(6)}_{3,k})\big) + w^{(6)}_{2,k} \\ x^{(6)}_{3,k+1} = x^{(6)}_{3,k} + \dfrac{dT}{A}\big(u'_{2,k} - q_2(x^{(6)}_{2,k}, x^{(6)}_{3,k}) - q_3(x^{(6)}_{3,k})\big) + w^{(6)}_{3,k} \\ x^{(6)}_{4,k+1} = x^{(6)}_{4,k} + w^{(6)}_{4,k} \\ y_{1,k} = x^{(6)}_{1,k} + v_{1,k} \\ y_{2,k} = x^{(6)}_{2,k} + v_{2,k} \\ y_{3,k} = x^{(6)}_{3,k} + x^{(6)}_{4,k} + v_{3,k} \end{cases}, \; x_0^{(6)} = \begin{bmatrix} x^{(6)}_{1,0} \\ x^{(6)}_{2,0} \\ x^{(6)}_{3,0} \\ x^{(6)}_{4,0} \end{bmatrix}.$$

Thereby, $x_k^{(0)} = [x_{1,k}\ x_{2,k}\ x_{3,k}]^T$, $w_k^{(0)} = [w_{1,k}\ w_{2,k}\ w_{3,k}]^T$, $x_k^{(6)} = [x_{1,k}\ x_{2,k}\ x_{3,k}\ \xi_k^{(6)}]^T$, $w_k^{(6)} = [w_{1,k}\ w_{2,k}\ w_{3,k}\ \lambda_k^{(6)}]^T$, and the flow rates q_{1-3} are determined according to (5.2). The corresponding (augmented) uncertainty models $\Omega^{(i)}$ are given as

$$\Omega^{(0)} \; := \; \left\{ \hat{\mathbb{X}}_0^{(0)} := \begin{Bmatrix} x_{1,0} \leq & |\bar{x}_{1,0}| \\ x_{2,0} \leq & |\bar{x}_{2,0}| \\ x_{3,0} \leq & |\bar{x}_{3,0}| \end{Bmatrix}, \; \mathbb{W}^{(0)} := \begin{Bmatrix} w_{1,k} \leq & |\bar{w}_1| \\ w_{2,k} \leq & |\bar{w}_2| \\ w_{3,k} \leq & |\bar{w}_3| \end{Bmatrix}, \; \mathbb{V} := \begin{Bmatrix} v_1 \leq & |\bar{v}_1| \\ v_2 \leq & |\bar{v}_2| \\ v_3 \leq & |\bar{v}_3| \end{Bmatrix} \right\}$$

$$\vdots$$

$$\Omega^{(6)} := \left\{ \hat{\mathbb{X}}_0^{(6)} := \left\{ \begin{array}{ll} x_{1,0} \leq & |\bar{x}_{1,0}| \\ x_{2,0} \leq & |\bar{x}_{2,0}| \\ x_{3,0} \leq & |\bar{x}_{3,0}| \\ \xi_0^{(6)} \leq & |\bar{\xi}_0^{(6)}| \end{array} \right., \ \mathbb{W}^{(6)} := \left\{ \begin{array}{ll} w_{1,k} \leq & |\bar{w}_1| \\ w_{2,k} \leq & |\bar{w}_2| \\ w_{3,k} \leq & |\bar{w}_3| \\ \lambda_k^{(6)} \leq & |\bar{\lambda}^{(6)}| \end{array} \right., \ \mathbb{V} := \left\{ \begin{array}{ll} v_1 \leq & |\bar{v}_1| \\ v_2 \leq & |\bar{v}_2| \\ v_3 \leq & |\bar{v}_3| \end{array} \right\}.$$

In order to gain an uncertainty representation that is compatible with the ellipsoidal representation employed by our robust FDI algorithm, the above uncertainty models have to be rewritten and approximated by ellipsoids. By utilizing an outer ellipsoidal approximation (with minimum volume), the uncertainty models are reformulated by seven ellipsoids (4.16), where

$$P_0^{(i)} = \frac{1}{n_x^{(i)}} \operatorname{diag}\left(\bar{x}_0^{(i)}\right)^{-2}, \ Q^{(i)} = \frac{1}{n_w^{(i)}} \operatorname{diag}\left(\bar{w}^{(i)}\right)^{-2}, \ R = \frac{1}{n_v} \operatorname{diag}\left(\bar{v}\right)^{-2} \tag{5.9}$$

are positive definite matrices defining the ellipsoidal shape. It is important to note that substitute ellipsoidal uncertainty representations may introduce additional conservatism. This applies particularly in the above exemplified case in which outer ellipsoids are used to express rectangular bounding sets. For a more extensive discussion of this approximate bounding procedure and the derivation of (5.9) the reader is referred to (Ros *et al.*, 2002).

5.2 Numerical Results

The numerical simulation is performed by using MATLAB/SIMULINK and the robust FDI is computed according to Algorithm 4.3 as

$$\text{rFDI}\left(\mathcal{S}_{\mathcal{U}}, \left\{u_\rho, y_\rho\right\}_0^k\right) = \hat{\mathbb{Z}}_k, \ k > M \tag{5.10}$$

employing a moving estimation window of length $M = 5$. The approach used to bound the approximation error due to the employed ESVE linearizations, is to use again the interval mathematics toolbox provided by Zemke. Table 5.2 summarizes the imposed fault-scenario and the fault characteristics.

Table 5.2: Overview of the performed test-scenario with $t_{\mathcal{F}}$ and $t_{\mathcal{H}}$ denoting the specific time of fault-occurrence and -recovery respectively.

Fault	Description	Maximum fault-magnitude	Unit	$t_{\mathcal{F}}, t_{\mathcal{H}}$ [s]
$\mathcal{F}_1$	Input-fault (actuator-fault) in pump 1	$\delta_{\max}^{(1)} = 2.0 \cdot 10^{-5}$	$[\text{m}^3/\text{s}]$	$100, 250$
$\mathcal{F}_2$	Output-fault (sensor-fault) in tank 1	$\delta_{\max}^{(2)} = 0.04$	[m]	$350, 500$
$\mathcal{F}_3$	Output-fault (sensor-fault) in tank 2	$\delta_{\max}^{(3)} = 0.04$	[m]	$600, 750$
$\mathcal{F}_4$	System-fault (leakage-fault) in tank 2	$\delta_{\max}^{(4)} = 3.0 \cdot 10^{-5}$	$[\text{m}^2]$	$850, 1000$
$\mathcal{F}_5$	Input-fault (actuator-fault) in pump 2	$\delta_{\max}^{(5)} = 2.0 \cdot 10^{-5}$	$[\text{m}^3/\text{s}]$	$1100, 1250$
$\mathcal{F}_6$	Output-fault (sensor-fault) in tank 3	$\delta_{\max}^{(6)} = 0.04$	[m]	$1350, 1700$
$\mathcal{F}_?$	Unknown multiple-fault $\mathcal{F}_1$ and $\mathcal{F}_6$	$- - - - - - - - - - - - -$	$- - -$	$1550, 1700$

5.2.1 Incipient Fault Scenario

Figure 5.3 shows the simulation results obtained when the faults $\mathcal{F}_1, \ldots, \mathcal{F}_6$ occur incipiently under the terms of the test sequence specified in Table 5.2. Figure 5.3 a) presents the normalized fault magnitudes that are subsequently imposed on the three-tank system. Starting from the fault-free condition with fault magnitudes equal zero, the imposed fault magnitudes increase continuously until their maximum values are reached. Between the times 1550 [s] and 1700 [s], the faults $\mathcal{F}_6$ and $\mathcal{F}_1$ affect the system simultaneously, hence the three-tank operates in an unanticipated multiple-fault mode, i.e., in the unknown mode.

According to the increasing fault magnitudes leaving their fault-free values, the true operating mode of the three-tank system changes abruptly, which is illustrated in Figure 5.3 b) by the gray

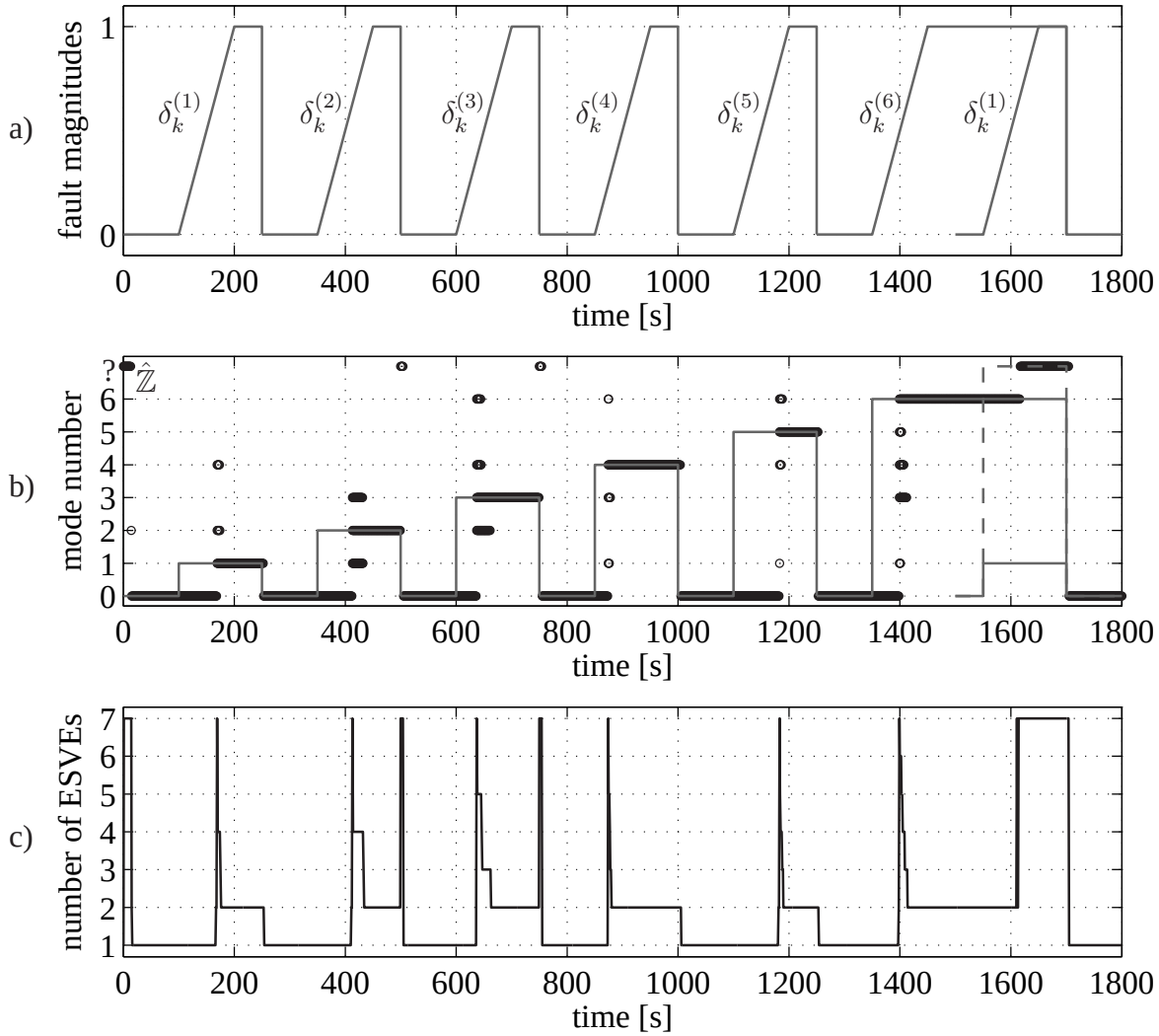


Figure 5.3: Robust FDI of the three-tank system operating subject to a sequence of incipient faults. a) Imposed (normalized) fault magnitudes. b) Imposed mode sequence (gray solid) and estimated set of modes (black circled). c) Number of simultaneously performed ESVEs.

line. Thereby, the multiple-fault mode (unknown mode) is identified by the gray dashed line. The plotted circles illustrate the set of estimated modes $\hat{\mathbb{Z}}_k$, i.e., the modes that are contained within. Starting from the initial mode $m_?$, the system is diagnosed immediately to operate in the fault-free mode initially. The first and also the subsequent faulty operations are detected with a certain delay and are uniquely isolated at the later time, in which the fault magnitudes exceed their critical thresholds (see Section 4.3.2.2). Between the respective time of the individual faults' detection and isolation, the estimated set of modes gradually scales down until the appropriate mode is uniquely isolated by the FDI function. Also with a slight delay, the unknown mode is isolated correctly. At the times 500 [s] and 750 [s], when the faults $\mathcal{F}_2$ and $\mathcal{F}_3$ are recovered and the three-tank returns to the fault-free operation, the FDI function temporarily passes into the unknown mode. Due to the abrupt decrease of the fault magnitudes and states, the fault-specific uncertainty models $\Omega^{(2)}$ and $\Omega^{(3)}$ (that merely allow "small" changes of the fault characteristics) are transiently invalidated, which results in a temporary isolation of the unknown mode. Of course, this effect could be eliminated by increasing the uncertainty bounds $\bar{\lambda}^{(2)}$ and $\bar{\lambda}^{(3)}$ - which, however, would entail a lower fault-sensitivity of the diagnosis function.

Figure 5.3 c) shows the number of ESVEs that are computed during the FDI procedure. The number of performed estimation-steps is time-variant and significantly underruns the constant number of seven estimators which would have been required to be calculated if using a classical estimator-bank approach. Hence, in off-line applications, a given I/O-sequence can be evaluated faster.

5.2.2 Abrupt Fault Scenario

Similar to the incipient fault case, Figure 5.4 shows the simulation results obtained when the faults $\mathcal{F}_1, \ldots, \mathcal{F}_6$ are imposed abruptly under the terms of our test sequence (Table 5.2). As before, Figure 5.4 a) presents the normalized fault magnitudes that subsequently affect the three-tank system. Between the times 1550 [s] and 1700 [s], the faults $\mathcal{F}_6$ and $\mathcal{F}_1$ affect the system simultaneously; causing again an unknown mode of operation.

Figure 5.4 b): Starting again from the initial mode $m_?$, the system is forthwith diagnosed to operate in the fault-free mode initially. The subsequent faulty operations and the unknown mode are now detected and isolated without delay since the abruptly changing fault magnitudes exceed their critical thresholds immediately. At the times of fault-occurrence and -recovery, the FDI function temporarily passes into the unknown mode for the same reason as above.

Figure 5.4 c) shows the time-variant number of ESVEs that are computed during the FDI procedure and shows also here the computational benefit in case that the switching FDI scheme is applied for the solution of off-line diagnosis problems.

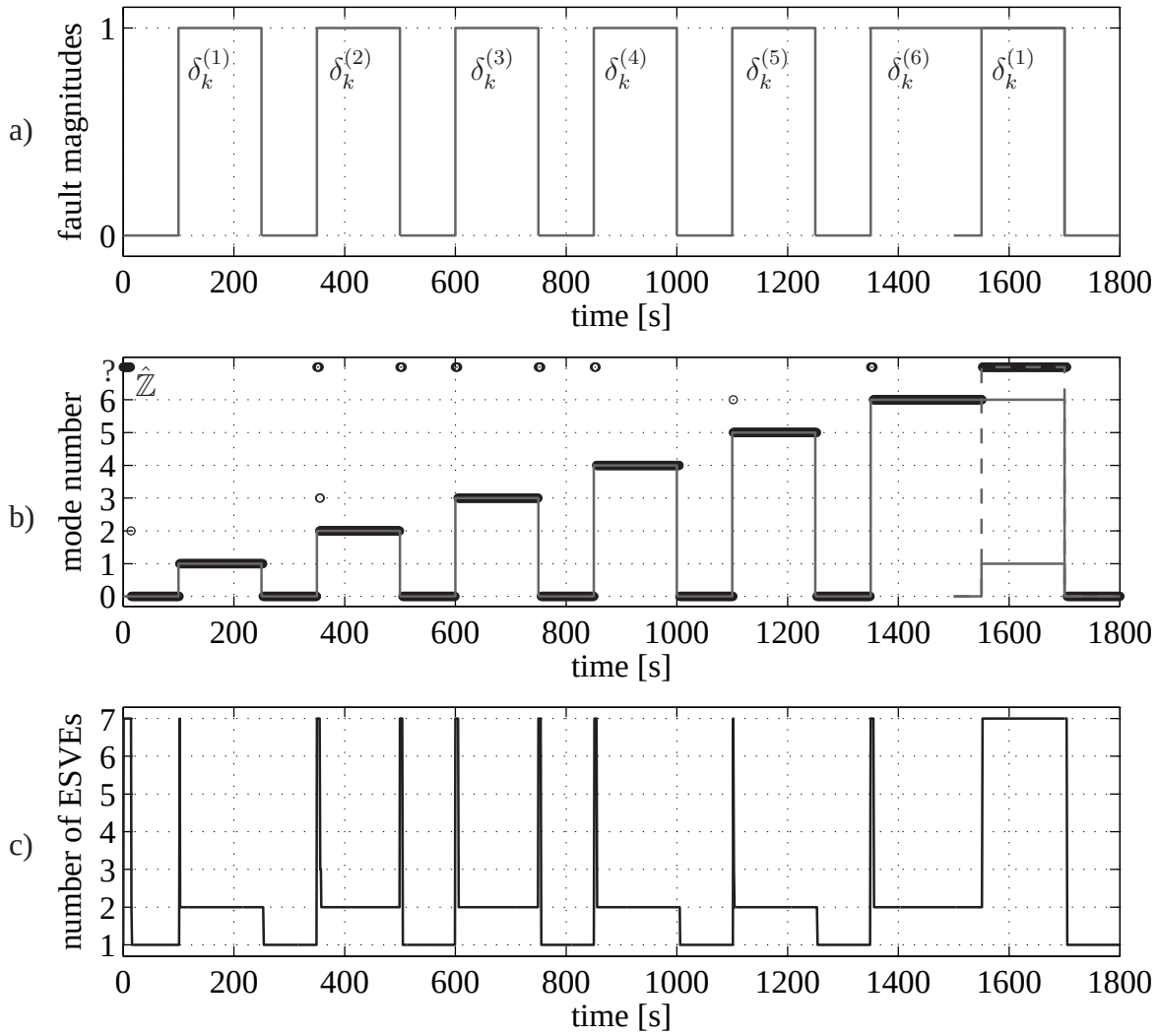


Figure 5.4: Robust FDI of the three-tank system operating subject to a sequence of abrupt faults. a) Imposed (normalized) fault magnitudes. b) Imposed mode sequence (gray solid) and estimated set of modes (black circled). c) Number of simultaneously performed ESVEs.

5.3 Summary

This chapter presents the robust FDI of the famous three-tank benchmark. It is shown that despite of the model uncertainty, a meaningful and robust FDI is determined. In other words, the estimated set of modes always contains the true operating mode of the three-tank and, thereby, is non-trivial since the estimated set of modes fades quickly to a unique isolation of the true mode. Particularly from the incipient fault case study, it is visible that the estimated set of modes becomes smaller if the fault magnitudes increase, until finally, a unique result is gained at the times, in which the fault magnitudes exceed their critical thresholds. Unanticipated operations of the three-tank (like inadmissable modeling uncertainties or unforeseen faults) do not lead to a unique false diagnosis; instead, the FDI function indicates an unknown operating mode.

By means of the three-tank benchmark, the remarkably wide applicability of the proposed FDI scheme is exemplified. To this, the configuration of the utilized problem setup is chosen such that a particularly general class of FDI applications is represented. It considers uncertain nonlinear systems, thereby uses as practical uncertainty description, allows to consider a large number of possible faults (of all commonly encountered types), and accounts for the unanticipated fault situation in which most of the present FDI methods fail. Thus, the provided FDI scheme is shown to be extremely versatile and to outperform a variety of sate-of-the-art FDI methods.

Chapter 6

Conclusions and Outlook

Summary

Most fault diagnosis problems as they appear in practice are nonlinear. Almost always, control engineers designing model-based algorithms for automated FDI have to rely on uncertain models that are due to disturbances, inexact system-knowledge, measurement noise, and unanticipated faults. In this thesis, the robust FDI of nonlinear systems under uncertainties is investigated. A comprehensive fault diagnosis scheme that embraces the modeling, the analysis and the robust FDI design for a general class of uncertain nonlinear diagnosis problems is presented. In this context, the thesis provides both novel and computationally tractable analysis conditions as well as robust FDI algorithms.

On the modeling side, the powerful and generally applicable formalism of structured augmented state modeling is introduced, which is suitable for representing nominal and uncertain nonlinear fault diagnosis problems. By utilizing the well proven state augmentation principle, the suggested formalism enables to bridge the methodical gap between the related fields of classical state observation and FDI theory. Additional constraints resulting from approved assumptions, like e.g. the well known single-fault assumption, are represented by means of a discrete-state automaton. The automaton specifies possible transitions between the fault-free and the faulty modes and enables a non-conservative representation of the underlying FDI problems.

Based on the suggested model, novel conditions for fault-detectability and -isolability are provided. The conditions prove the gain of observability as originally intended by the introduction of the structured augmented state modeling paradigm. Furthermore, the derived conditions are extraordinarily suited for fault-detectability and -isolability analysis. Because both conditions can be practically checked by means of known observability analysis methods, these are particularly useful and significantly extend the current repertoire of analysis methods in FDI.

Synthesis of FDI algorithms is addressed in various ways. In the nominal setup, the diagnosis problem is expressed as a hybrid state estimation problem and the optimal but computationally in-

tractable solution is outlined as a reference. The use of modern sub-optimal hybrid estimation approaches is motivated and illustrated for a DC actuator example. For the uncertain problem setup, a comprehensive and theoretically sound approach to robust FDI is developed. As in the nominal case, an ideal but computationally intractable solution to the robust FDI problem is derived firstly and then subsequently relaxed to an approximate but practically useful approach. Besides a rather simple FDI scheme being suited for tackling non-switching diagnosis problems, a novel robust FDI algorithm is provided, which is also capable to come up with switching cases appearing, e.g., when intermittent faults are due. Another outstanding feature of the general robust FDI scheme is its unknown mode capability which, under certain conditions, enables the isolation of unanticipated faults. New robust fault detection and isolation conditions complete the results. Provided that these conditions hold, the proposed algorithms are guaranteed to determine a non-trivial and robust FDI. The conditions disclose the inherent tradeoff between the attainable fault-sensitivity and the robustness of the provided FDI algorithms. Hence, this work provides a comprehensive setup of methods for the modeling, analysis, and design of robust nonlinear FDI functionalities and contributes to the important field of application oriented FDI.

Outlook

Several promising extensions of the suggested robust FDI design are thinkable. On the one hand, the presented robust FDI method can be further improved by enhancing the included set-valued estimation algorithms. The use of more accurate approximations for the nonlinearities, the state-, and the uncertainty-sets may further help to reduce possible conservatism. For instance, linearization error effects could be minimized by enhancing higher-order Kalman filter approaches (e.g. the unscented Kalman filter (Julier *et al.*, 2000; Julier and Uhlmann, 2004) or the second-order divided difference filter (Norgaard *et al.*, 2000)) and transferring them into the underlying ellipsoidal set-valued estimation framework. On the other hand, alternative problem-specific set-representation techniques may be used in order to provide for less conservative descriptions of the crucial state- and uncertainty-sets. Furthermore, an extension of the considered system class to hybrid systems is thinkable due to the already hybrid character of the proposed framework. Another promising advancement of the provided FDI approach is its further development towards fault tolerant control applications.

Bibliography

Ackerson, G. and K. Fu (1970). On state estimation in switching environments. *IEEE Transactions on Automatic Control* **15**, 10–16.

Aeyels, D. (1981). Generic observability of differentiable systems. *Siam. J. Contr. Optim.* **19**, 595–603.

Aßfalg, J. and F. Allgöwer (2006*a*). Fault diagnosis of constrained nonlinear systems using structured augmented state models. In: *Proc. of the IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS)*. pp. 1375–1380.

Aßfalg, J. and F. Allgöwer (2006*b*). Fault diagnosis with structured augmented state models: Modeling, analysis, and design. In: *Proc. of the IEEE Conference on Decision and Control (CDC)*. pp. 1165–1170.

Aßfalg, J. and F. Allgöwer (2007). Fault diagnosis of nonlinear systems using structured augmented state models. *International Journal of Automation and Computing* **4**, 141–148.

Aßfalg, J., F. Allgöwer and M. Fritz (2006). Constrained derivative-free augmented state estimation for a diesel engine air path. In: *Proc. of the IFAC Symposium on System Identification (SYSID)*. pp. 1382–1387.

Alamo, T., J. M. Bravo and E. F. Camacho (2003). Guaranteed state estimation by zonotopes. In: *Proc. of the IEEE Conference on Decision and Control*. pp. 5831–5836.

Alamo, T., J.M. Bravo and E.F. Camacho (2005). Guaranteed state estimation by zonotopes. *Automatica* **41**, 1035–1043.

Aschemann, H., O. Sawodny, S. Lahres and E. P. Hofer (2000). Disturbance estimation and compensation for trajectory control of an overhead crane. In: *Proc. American Control Conf. (ACC)*. pp. 1027–1031.

Ballé, P. (2002). *Modellbasierte Fehlererkennung für nichtlineare Prozesse mit linear parameterveränderlichen Modellen*. VDI Verlag GmbH. Düsseldorf.

Bar-Shalom, Y. and X. R. Li (1993). *Estimation and Tracking - Principles, Techniques and Software*. Artech House. Boston, London.

Bertsekas, D. P. and I. B. Rhodes (1971). Recursive state estimation for a set-membership description of uncertainty. *IEEE Transactions on Automatic Control* **16**, 117–128.

Birk, J. (1992). Rechnergestützte Analyse und Lösung nichtlinearer Beobachtungsaufgaben. PhD thesis. Univ. of Stuttgart. Stuttgart.

Blanke, M. (1999). Fault tolerant control systems. In: *Advances of Control: Highlights of ECC'99* (P. M. Frank, Ed.). Chap. 6. Springer-Verlag.

Blanke, M., M. Kinnaert, J. Lunze and M. Staroswiecki (2003). *Diagnosis and Fault-Tolerant Control*. Springer-Verlag. Berlin, Heidelberg.

Blom, H. A. and Y. Bar-Shalom (1988). The interacting multiple model algorithm for systems with markovian switching coefficients. *IEEE Transactions on Automatic Control* **33**, 780–783.

Boutayeb, M., H. Rafaralahy and M. Darouach (1997). Convergence analysis of the extended Kalman filter used as an observer for nonlinear deterministic discrete-time systems. *IEEE Transactions on Automatic Control* **42**, 581–586.

Buja, G. S., R. Menis and M. I. Valla (1995). Disturbance torque estimation in a sensorless dc drive. *IEEE Transactions on Industrial Electronics* **42**, 351–357.

C. De Persis and A. Isidori (1999). On the problem of residual generation for fault detection in nonlinear systems and some related facts. In: *Proc. of the European Control Conference (ECC)*.

Caglayan, A. K. (1980). Necessary and sufficient conditions for detectability of jumps in linear systems. *IEEE Transactions on Automatic Control* **25**, 833–834.

Cassandras, C. G. and S. Lafortune (1999). *Introduction to Discrete Event Systems*. Kluwer Academic Publishers. Boston, Dordrecht, London.

Chen, J. and R. J. Patton (1999). *Robust Model-Based Fault Diagnosis for Dynamic Systems*. Kluwer. Boston MA.

Chernousko, F. L. (2004). *State Estimation for Dynamic Systems*. CRC-Press. Boca Raton.

Chisci, L., A. Garulli and G. Zappa (1996). Recursive state bounding parallelotopes. *Automatica* **32**, 1049–1055.

Clark, R. N. (1979). The dedicated observer approach to instrument fault detection. In: *Proc. of the IEEE Conference on Decision and Control (CDC)*. pp. 237–241.

Cox, H. (1964). On the estimation of state variables and parameters for noisy dynamic systems. *IEEE Transactions on Automatic Control* **9**, 5–12.

De Kleer, J. and B. C. Williams (1987). Diagnosing multiple faults. *Artificial Intelligence* **32**, 97–130.

De Kleer, J. and B. C. Williams (1989). Diagnosis with behavioral modes. In: *Proc. of the International Joint Conference on Artificial Intelligence*. pp. 1324–1330.

Ding, S. X. (2008). *Model-Based Fault Diagnosis Techniques*. Springer. Berlin.

Ding, S. X., P. Zhang, E. L. Ding and P. M. Frank (2003). Study on detecting multiplicative faults in linear dynamic systems. In: *Proc. of the American Control Conference (ACC)*. pp. 1776–1781.

Ducard, G. and H. P. Geering (2006). A reconfigurable flight control system based on the EMMAE method. In: *Proc. of the American Control Conference (ACC)*. pp. 5499–5504.

Farrell, J. A., T. Berger and B. D. Appleby (1993). Using learning techniques to accomodate unantcipated faults. *IEEE Control Systems Magazine* **13**, 40–49.

Findeisen, R., L. Imsland, F. Allgöwer and B. Foss (2003). Towards a sampled-data theory for nonlinear model predictive control. In: *New Trends in Nonlinear Dynamics and Control* (W. Kang, C. Borges and M. Xiao, Eds.). pp. 295–313. Lecture Notes in Control and Information Sciences. Springer-Verlag. New York.

Frank, P. M. (1994). On-line fault detection in uncertain nonlinear systems using diagnostic observers: A survey. *International Journal of Systems Science* **25**, 2129–2154.

Garica, E. A. and P. M. Frank (1999). Multiplicative fault isolation in linear systems. In: *Proc. of the IEEE Conference on Decision and Control (CDC)*. pp. 3114–3115.

Garulli, A. and A. Vicino (2001). A set-membership localization of mobile robots via angle measurements. *IEEE Transactions on Robotics and Automation* **17**, 450–463.

Gelb, A., J. F. Kasper, R. A. Nash, C. F. Price and A. A. Sutherland (1974). *Applied Optimal Estimation*. The M.I.T. Press. Cambridge, Massachussets, and London, England.

Gertler, J. and D. Singer (1990). A new structural framework for parity equation based failure detection and isolation. *Automatica* **26**, 381–388.

Gertler, J. J. (1988). Survey of model-based failure detection and isolation in complex plants. **8**, 3–11.

Gertler, J. J. (1998). *Fault Detection and Diagnosis in Engineering Systems*. Marcel Dekker, Inc.. New York, Basel.

Gertler, J., X. Fang and Q. Luo (1990). Detection and diagnosis of plant failures: The orthogonal parity equation approach. *Control and Dynamic Systems* **37**, 159–216.

Hammouri, H., M. Kinnaert and E. H. El Yaagoubi (1999). Application of nonlinear observers to fault detection and isolation. In: *New Directions in Nonlinear Observer Design* (H. Nijmeijer and T. I. Fossen, Eds.). pp. 423–443. Springer-Verlag. Berlin.

Hamscher, W. (1992). In: *Readings in Model Based Diagnosis* (L. Console and J. De Kleer, Eds.). Morgan Kaufmann.

Hansen, E. (1992). *Global Optimization Using Interval Analysis*. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker.

Hermann, R. and A. J. Krener (1977). Nonlinear controllability and observability. *IEEE Transactions on Automatic Control* **22**, 728–740.

Hofbaur, M. W. (2005). *Hybrid Estimation of Complex Systems*. Springer-Verlag. Berlin, Heidelberg.

Hofbaur, M. W. and B. C. Williams (2004). Hybrid estimation of complex systems. *IEEE Transactions on Systems, Man, and Cybernetics* **34**, 2178–2191.

Inouye, Y. (1977). On the observability of autonomous nonlinear systems. *Journal of Mathematical Analysis and Applications* **60**, 236–274.

Isermann, R. (1989). Beispiele für die Fehlerdiagnose mittels Parameterschätzung. *Automatisierungstechnik* **37**, 336–343.

Isermann, R. (1994). *Überwachung und Fehlerdiagnose - Moderne Methoden und ihre Anwendung bei technischen Systemen*. VDI Verlag. Düsseldorf.

Isermann, R. (1997). Supervision, fault detection, and fault diagnosis methods - An introduction. *Control Engineering Practice* **5**, 639–652.

Isidori, A., L. Marconi and A. Serrani (2004). *Robust Autonomous Guidance: An Internal Model Approach*. Springer Verlag. London.

Jaulin, L. and E. Walter (1993). Set inversion via interval analysis for nonlinear bounded-error estimation. *Automatica* **29**, 1053–1064.

Join, C., J. C. Ponsart, D. Sauter and D. Theilliol (2005). Nonlinear filter design for fault diagnosis: Application to the three-tank system. *IEE Proc. Control Theory Appl.* **152**, 55–64.

Julier, S. J. and J. K. Uhlmann (1997). A new extension of the Kalman filter to nonlinear systems. *Proc. AeroSense 11th Int. Symp. Aerospace/Defense Sensing, Simulation and Controls* pp. 182–193.

Julier, S. J. and J. K. Uhlmann (2004). Unscented filtering and nonlinear estimation. *Proc. of the IEEE* **92**, 401–422.

Julier, S. J., J. K. Uhlmann and H. F. Durrant-Whyte (2000). A new method for the nonlinear transformation of means and covariances in filters and estimators. *IEEE Transactions on Automatic Control* **45**, 477–482.

Kailath, T. (1980). *Linear Systems*. Prentice Hall. Englewood Cliffs.

Kieffer, M., L. Jaulin and E. Walter (1998). Guaranteed recursive nonlinear state estimation with optimal bounding ellipsoids. In: *Proc. of the IEEE Conference on Decision and Control*. pp. 3966–3971.

Kinnaert, M. (1999). Robust fault detection based on observers for bilinear systems. *Automatica* **35**, 1829–1842.

Kou, S. R., D. L. Elliot and T. J. Tarn (1973). Observability of nonlinear systems. In: *Information and Control*. pp. 89–99.

Köppen-Seliger, B., E. A. Garcia and P.M. Frank (1999). Fault Detection: Different strategies for modelling applied to the three tank benchmark - A case study. In: *Proc. of the European Control Conference (ECC)*.

Kurzhanski, A. B. and I. Vályi (1997). *Ellipsoidal Calculus for Estimation and Control*. Birkhäuser. Boston, Basel, Berlin.

Kurzhanski, A. B. and V. M. Veliov (1993). *Modeling Techniques for Uncertain Systems*. Birkhäuser. Boston.

Kwan, C. and R. Xu (2004). A note on simultaneous isolation of sensor and actuator faults. *IEEE Transactions on Control Systems Technology* **12**, 183–192.

Leonhard, W. (2001). *Control of Electrical Drives*. Springer-Verlag. Berlin - Heidelberg - New York.

Li, W. and J. Jiang (2004). Isolation of parametric faults in continuous-time multivariate systems: A sampled data-based approach. *Journal of Process Control* **77**, 173–187.

Li, W. and S. Shah (2002). Structured residual vector-based approach to sensor fault detection and isolation. *Journal of Process Control* **12**, 429–443.

Li, X. R. and Y. Bar-Shalom (1996). Multiple-model estimation with variable structure. *IEEE Transactions on Automatic Control* **41**, 478–493.

Liu, T. S. and J. J. Liou (1995). An augmented system model for fault detection and identification. In: *Proc. American Control Conference (ACC)*. pp. 602–606.

Lunze, J. (2003). *Automatisierungstechnik: Methoden für die Überwachung und Steuerung kontinuierlicher und ereignisdiskreter Systeme*. Oldenbourg. München, Wien.

Mhaskar, P., A. Gani, N.H. El-Farra, C. McFall, P.D. Christofides and J.F. Davis (2006). Integrated fault-detection and fault-tolerant control for process systems. *AIChE Journal* **52**, 2129–2148.

Milanese, M. and V. Vicino (1991). Optimal estimation theory for dynamic systems with set-membership uncertainty: An overview. *Automatica* **27**, 997–1009.

Moore, R. E. (1966). *Interval Analysis*. Prentice Hall.

Muske, K. R. and J. B. Rawlings (1995). Nonlinear moving horizon state estimation. In: *Methods of Model Based Process Control* (R. Berber, Ed.). Kluwer Academic Publishers. The Netherlands.

Muske, K. R. and T. F. Edgar (1997). Nonlinear state estimation. In: *Nonlinear Process Control* (D. E. Seborg, Ed.). Prentice Hall. Englewood Cliffs, NJ.

Nguang, S. K., P. Zhang and S. X. Ding (2007). Parity relation based fault estimation for nonlinear systems: An LMI approach. *International Journal of Automation and Computing* **4**, 164–168.

Nijmeijer, H. (1982). Observability of autonomous discrete-time nonlinear systems: A geometric approach. *International Journal of Control* **36**, 867–874.

Nijmeijer, H. and A. J. Van der Schaft (1990). *Nonlinear Dynamical Control Systems*. Springer-Verlag. Berlin.

Norgaard, M., N. K. Poulsen and O. Ravn (2000). Advances in derivative-free state estimation for nonlinear systems. *Technical Report, IMM-REP-1998-15, Department of Mathematical Modelling, DTU, revised April*.

Nyberg, M. (2003). Model based fault diagnosis using structured hypothesis tests. *Proc. of the IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS)* pp. 1026–1031.

Nyberg, M. and L. Nielsen (2000). A universal Chow-Willsky scheme and detectability criteria. *IEEE Transactions on Automatic Control* **45**, 152–156.

Petersen, I.R. and A.V. Savkin (1999). *Robust Kalman Filtering for Signals and Systems with Large Uncertainties*. Birkhäuser. Boston.

Polyak, B.T., S.A. Nazin, C. Durieu and E. Walter (2004). Ellipsoidal parameter or state estimation under model uncertainty. *Automatica* **40**, 1171–1179.

Ramesh, T. S., J. F. Davis and G. M. Schwenzer (1992). Knowledge-based diagnostic systems for continuous process operations based upon the task framwork. *Computers and Chemical Engineering* **16**, 109–127.

Rao, C. V. and J. B. Rawlings (2000). Nonlinear moving horizon state estimation. In: *Nonlinear Model Predictive Control* (F. Allgöwer and A. Zheng, Eds.). Birkhäuser Verlag. Basel - Boston - Berlin.

Rao, C. V., J. B. Rawlings and D. Q. Mayne (2003). Constrained state estimation for nonlinear discrete-time systems: Stability and moving horizon approximations. *IEEE Transactions on Automatic Control* **48**, 246–258.

Ros, L., A. Sabater and F. Thomas (2002). An ellipsoidal calculus based on propagation and fusion. *IEEE Transactions On Systems, Man, and Cybernetics* **32**, 430–442.

Rupp, D., G. Ducard, E. Shafai and H. P. Geering (2005). Extended multiple model adaptive estimation for the detection of sensor and actuator faults. In: *Proc. of the IEEE Conference on Decision and Control (CDC)*. pp. 3079–3084.

Sampath, M., R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control* **40**, 1555–1575.

Savkin, A. V. and I. R. Petersen (1997). New approach to model validation and fault diagnosis. *Journal of Optimization Theory and Applications* **94**, 241–250.

Savkin, A. V. and I.R. Petersen (1995). A new approach to model validation and fault diagnosis. In: *Proc. of the European Control Conference (ECC)*. pp. 1418–1422.

Scholte, E. and M. E. Campbell (2002). On-line nonlinear guaranteed estimation with application to a high performance aircraft. In: *Proc. of the American Control Conference (ACC)*. pp. 184–190.

Scholte, E. and M. E. Campbell (2003). A nonlinear set-membership filter for on-line applications. *International Journal of Robust and Nonlinear Control* **13**, 1337–1358.

Schröder, J. (2003). *Modelling, State Observation, and Diagnosis of Quantised Systems*. Springer-Verlag. Berlin, Heidelberg, New York.

Schweppe, F. C. (1968). Recursive state estimation: Unknown but bounded errors and system inputs. *IEEE Transactions on Automatic Control* **13**, 22–28.

Shamma, J. S. and K. Y. Tu (1997). Approximate set-valued observers for nonlinear systems. *IEEE Transactions on Automatic Control* **42**, 648–658.

Shamma, J. S. and K. Y. Tu (1999). Set-valued observers and optimal disturbance rejection. *IEEE Transactions on Automatic Control* **44**, 253–264.

Shumsky, A. and M. Staroswiecki (2003). Fault detectability and isolability for nonlinear uncertain systems. *Proc. of the IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS)* pp. 639–644.

Simani, S., C. Fantuzzi and R.J. Patton (2002). *Model-based Fault Diagnosis in Dynamic Systems Using Identification Techniques*. Springer-Verlag. London.

Staroswiecki, M. and B. Darkhovski (2001). On structural and parity space detectability. In: *Proc. of the European Control Conference (ECC)*. pp. 1970–1974.

Stoustrup, J. and H. Niemann (1999). Fault detection and isolation systems with parametric faults. In: *Proceedings of the 14th IFAC World Congress*. pp. 717–729.

Stoustrup, J. and H. Niemann (2006). Fault isolability conditions for linear systems with additive faults. In: *Proc. of the American Control Conference (ACC)*. pp. 2345–2350.

Tanaka, S. (1989). Diagnosability of systems and optimal sensor location. In: *Fault Diagnosis in Dynamic Systems* (R. J. Patton, P. M. Frank and R. Clark, Eds.). Prentice Hall International. London (UK).

Tsakalis, K.S. and L. Song (1994). Set-membership estimation for weakly nonlinear models: An application to the adaptive control of semiconductor manufactoring processes. In: *Proc. of the IEEE Conference on Decision and Control*. pp. 1066–1071.

Tyler, M. L., K. Asano and M. Morari (2000). Application of moving horizon estimation based fault detection to cold tandem steel mill. *International Journal of Control* **73**, 427–438.

Ushio, T., I. Onishi and K. Okuda (2003). Fault detection based on petri net models with faulty behaviors. In: *Proc. of the IEEE Conference on Systems, Man and Cybernetics*. pp. 113–118.

Venkatasubramanian, V., R. Rengaswamy and S. N. Kavuri (2003*a*). A review of process fault detection and diagnosis Part II: Qualitative models and search strategies. *Computers and Chemical Engineering* **27**, 313–326.

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

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

Viswanadham, N. and R. Srichander (1987). Fault detection using unknown-input observers. *Control Theory and Advanced Technology* **3**, 91–101.

Whiteley, J. R. and J. F. Davis (1992). Knowledge-based interpretation of sensor patterns. *Computers and Chemical Engineering* **16**, 329–346.

Young, P. (1981). Parameter estimation for continuous time models - a survey. *Automatica* **17**, 23–29.

Zhang, X., M. M. Polycarpou and T. Parisini (2002). A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems. *IEEE Transactions on Automatic Control* **47**, 576–593.

Zhang, X., T. Parisini and M. Polycarpou (1999). Robust parametric fault detection and isolation for nonlinear systems. In: *Proceedings of the 38th IEEE Conference on Decision and Control (CDC)*. pp. 3102–3107.

Zimmermann, W. and R. Schmidgall (2008). *Bussysteme in der Fahrzeugtechnik - Protokolle und Standards*. Vieweg-Verlag.