HAL open science

Diagnostique de défaut à base de modèle et accommodation de défaut pour missions spatiales

Robert Fonod

To cite this version:

Robert Fonod. Diagnostique de défaut à base de modèle et accommodation de défaut pour missions spatiales. Physics [physics]. Université de Bordeaux, 2014. English. NNT : 2014BORD0199 . tel-01163681

HAL Id: tel-01163681

https://theses.hal.science/tel-01163681v1

Submitted on 15 Jun 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THÈSE

présentée pour obtenir le grade de

Docteur de l'Université de Bordeaux

ÉCOLE DOCTORALE DES SCIENCES PHYSIQUES ET DE L'INGENIEUR

SPÉCIALITÉ : Automatique, Productique, Signal et Image, Ingénierie Cognitique

par

Robert FONOD

Model-based Fault Diagnosis and Fault Accommodation for Space Missions

Application to the Rendezvous Phase of the MSR Mission

Présentée et soutenue publiquement le 19 Novembre 2014

Après avis de :

Prof. Mogens BLANKE	Université Technique du Danemark, Copenhague
Prof. Didier THEILLIOL	Université de Lorraine, CRAN, Nancy

Devant la commission d'examen formée de :

Prof. David HENRY	Université de Bordeaux, IMS-CNRS, Bordeaux	Direct. de thèse
Prof. Mogens BLANKE	Université Technique du Danemark, Copenhague	Rapporteur
Prof. Didier THEILLIOL	Université de Lorraine, CRAN, Nancy	Rapporteur
Prof. András EDELMAYER	Académie Hongroise des Sciences, SZTAKI, Budapest	Examinateur
Prof. Ali ZOLGHADRI	Université de Bordeaux, IMS-CNRS, Bordeaux	Examinateur
Dr. Samir BENNANI	Agence Spatiale Européenne, ESA/ESTEC, Noordwijk	Examinateur
Dr. Damiana LOSA	Thales Alenia Space, Cannes	Examinateur
Dr. Eric BORNSCHLEGL	Agence Spatiale Européenne (retraité)	Examinateur

- 2014 -

THESIS

submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy from University of Bordeaux

DOCTORAL SCHOOL OF PHYSICAL SCIENCES AND ENGINEERING

SPECIALISM: Automatic, Production Engineering, Signal and Image Processing, Cognitive Engineering

by

Robert FONOD

Model-based Fault Diagnosis and Fault Accommodation for Space Missions

Application to the Rendezvous Phase of the MSR Mission

Presented and publicly defended the 19th of November 2014

After review by:

Prof. Mogens BLANKE	Technical University of Denmark - DTU, Copenhagen
Prof. Didier THEILLIOL	University of Lorraine, CRAN, Nancy

To the examining committee composed of:

Prof. David HENRY	University of Bordeaux, IMS-CNRS, Bordeaux	Thesis supervisor
Prof. Mogens BLANKE	Technical University of Denmark - DTU, Copenhagen	Reviewer
Prof. Didier THEILLIOL	University of Lorraine, CRAN, Nancy	Reviewer
Prof. András EDELMAYER	Hungarian Academy of Sciences, SZTAKI, Budapest	Examiner
Prof. Ali ZOLGHADRI	University of Bordeaux, IMS-CNRS, Bordeaux	Examiner
Dr. Samir BENNANI	European Space Agency, ESA/ESTEC, Noordwijk	Examiner
Dr. Damiana LOSA	Thales Alenia Space, Cannes	Examiner
Dr. Eric BORNSCHLEGL	European Space Agency (retiree)	Examiner

- 2014 -

"In order to be a realist you must believe in miracles."

— David Ben-Gurion, first prime minister of Israel

"Do not follow the ideas of others, but learn to listen to the voice within yourself."

— Eihei Dōgen, Zen master

Acknowledgements

I would like to thank the Guidance, Navigation and Control (GNC) section at the European Space Research and Technology Centre (ESTEC) of the European Space Agency (ESA) and the Research and Technology/Science and Observation within the R&D department (DRT/SO) at Thales Alenia Space France (TAS-F) for providing the funding that made this research possible, through the ESA's Networking/Partnering Initiative (NPI) Program.

A quotation goes that "***a journey is always easier when you travel together***", and we really have travelled together! During my PhD study, I have been accompanied and supported by many. It is my great pleasure to take this opportunity to express my sincere gratitude to all of them. First and foremost, I would like to thank my supervisor, Prof. D. Henry from University of Bordeaux, for his continuous and generous support, patience, encouragement, understanding and valuable time. By providing the right balance of suggestions and freedom, as well as the wonderful discussions on all aspects of this work, he has made this work not just possible, but more importantly, enjoyable! His excellent guidance and profound appreciation of the topic, helped me in all phases of the research and writing of this thesis. It has been a honour and a great pleasure to work with him, Merci David !

At ESTEC, my special thanks go to Dr. E. Bornschlegl for his hearty welcome and hospitality during my six months stay in the Netherlands, proof-reading my papers, sharing his travel experiences and giving me practical advices for life. I would also like to acknowledge Dr. S. Bennani for being part of the examining committee and for his perceptive comments. Many thanks also go to Dr. G. Ortega, Dr. A. Benoit and other members of ESA TEC-ECN/ECC, for their support during my stay in ESTEC.

At TAS-F, I would first like to thank Dr. C. Charbonnel for welcoming me to DRT/SO and for helping me to direct my research from industrial aspects. Thanks go to Dr. D. Losa for her careful reading of the manuscript and for the many useful comments and suggestions which allowed to improve the style of the manuscript. Special thanks also to my officemate Jonathan, for his valuable inputs and constructive discussions. I would also like to thank them for their friendship and assistance with all the issues and making my stay in Cannes an enjoyable one.

I have been fortunate to work two years in the pleasant atmosphere of the IMS (laboratoire de l'Intégration du Matériau au Système) laboratory at the University of Bordeaux. Therefore, I would like to thank all the members and staff of the lab for their support. Especially, Prof. A. Zolghadri is acknowledged for letting me join his ARIA (Approche Robuste et Intégrée de l'Automatique) research team, for the interactions during the whole period and invitations to

various events. I also thank Prof. Zolghadri for serving as the president of the thesis examination committee and for his final quotation ("*The dogmas of the quiet past, are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew. We must disenthrall ourselves, and then we shall save our country.*" — Abraham Lincoln), uttered after the the deliberation of my doctoral degree.

I am also very grateful to Prof. M. Blanke from DTU and Prof. D. Theilliol from University of Lorraine for their precious time to review my thesis, and for their insightful comments which allowed to improve the quality of the final manuscript.

I must especially thank two men without whom I would have never started this adventure: Prof. A. Edelmayer from Hungarian Academy of Sciences, who was the first to believe in my ability to conduct this work, and Prof. D. Krokavec with whom I discovered my interest in research while at the Technical University of Kosice. I also thank Prof. Krokavec for introducing me to the wonderful world of fault diagnosis, for his lectures, constant support and keeping in touch during my studies.

Thanks also goes to all my fellow colleagues at IMS lab (Valentin, Souad, Daniela, Alejandra, Roxana, Andrei and Ayat) and at ESTEC (Julien, Guillaume, and many more) for inspiring working atmosphere and nice coffee breaks.

On a personal level, many have supported me along the way. First and foremost, my parents, brother and sisters have all guided and influenced me in their own way. I am grateful to Miriam for her continuous support, understanding, patience and encouragements during all these years.

Slovakia, December 2014 Robert Fonod

Table of Contents

Acknowledgements **i**

Table of Contents **iii**

List of Figures **vii**

List of Tables **xi**

Nomenclature **xiii**

Terminology **xix**

Author's List of Publications **xxiii**

Résumé en Français (French Summary) **xxv**

Introduction **1**

1 State of the Art in Model-based Fault Diagnosis and Active FTC **7**

1.1 Introduction . . . 7
1.2 General Procedure of Fault-tolerant Control Systems . . . 8
1.3 Methods for Fault Detection and Isolation . . . 12
1.3.1 Parity Space Approach . . . 12
1.3.2 Observer-based Approaches . . . 15
1.3.2.1 Iterative Learning Observer . . . 16
1.3.2.2 Unknown Input Observer . . . 16
1.3.2.3 Eigenstructure Assignment . . . 20
1.3.2.4 Sliding Mode Observers . . . 23
1.3.2.5 Geometric Approaches . . . 25
1.3.3 Parameter Identification-based Approaches . . . 29
1.3.3.1 Extended Kalman Filter . . . 30
1.3.3.2 Particle Filtering . . . 31
1.3.3.3 Unscented Kalman Filter . . . 33
1.3.4 Norm-based Approach . . . 35
1.3.4.1 The Pure H_∞ Filtering Formulation . . . 35
1.3.4.2 The H_∞/H_- Approach . . . 37

1.3.5 Decision Test . . . 45
1.3.6 Fault Isolation . . . 47
1.3.7 Fault Identification . . . 50
1.4 Active Fault-tolerant Control Approaches . . . 50
1.4.1 Projection-based Paradigm . . . 51
1.4.1.1 Multiple-Model Approach . . . 51
1.4.1.2 Bank of Observers for Sensor Faults . . . 54
1.4.2 Automatic Design . . . 55
1.4.2.1 On-line Controller Re-design . . . 55
1.4.2.2 Fault-hiding Paradigm . . . 61
1.4.3 Control Allocation . . . 62
1.4.3.1 The Control Allocation Problem . . . 63
1.4.3.2 Control Allocation Methods . . . 64
1.4.3.3 Control Allocation for Fault-tolerant Control . . . 66
1.4.4 Enhanced and New Theories in FTC . . . 67
1.4.4.1 The Supervisory FTC Approach . . . 67
1.4.4.2 The Trajectory Re-planning Approach . . . 69
1.5 Conclusion . . . 70
1.5.1 Summary of the FDI/FDD Approaches . . . 70
1.5.2 Summary of the FTC Approaches . . . 71

2 MSR Mission Description and Modelling 73
2.1 Overview of the MSR Mission . . . 73
2.1.1 Terminal Rendezvous Phase . . . 75
2.2 Chaser Spacecraft GNC . . . 76
2.2.1 Sensors and Navigation Modelling Issues . . . 77
2.2.1.1 LIDAR Modelling Issues . . . 78
2.2.1.2 Attitude Quaternion Modelling Issues . . . 78
2.2.1.3 Angular Rate Measurement Model . . . 79
2.2.2 Translation and Attitude Guidance . . . 79
2.2.3 Control and Actuator Management Functions . . . 82
2.2.3.1 Attitude Control Loop . . . 83
2.2.3.2 Position Control Loop . . . 86
2.2.3.3 Robustness Margins and Performances . . . 88
2.2.3.4 Actuator Management Functions . . . 89
2.3 Failure Management and Fault Considerations . . . 91
2.3.1 Description of the Set of Detection Functions at the Subsystem Level . . 93
2.3.2 Description of the Set of Detection Functions at the Safety Monitoring Level 97
2.3.3 Thruster Fault Modelling . . . 98
2.4 Modelling the Chaser Dynamics during the Rendezvous Phase . . . 99
2.4.1 Relative Position Model . . . 99
2.4.2 Attitude Model . . . 101
2.5 Conclusion . . . 103

3 Advanced Model-based FDIR Solution for the Baseline MSR Thruster Configuration 105
3.1 Problem Statement and Motivation . . . 105
3.2 Robust FDI Scheme Design . . . 109

3.2.1 Overview of the Time-delay Problematic . . . 109
3.2.2 Problem Formulation . . . 110
3.2.3 Uncertainty Transformation . . . 113
3.2.3.1 Uncertainty Transformation Using Cayley-Hamilton Theorem . . 114
3.2.3.2 Uncertainty Transformation Using Taylor Series Expansion . . . 115
3.2.4 Approximation of the Uncertainty in Terms of Unknown Inputs . . . 117
3.2.5 Residual Generator Design with Decoupled Unknown Inputs . . . 118
3.2.5.1 Left Eigenstructure Assignment . . . 120
3.2.6 Computational Procedure and Comments on Implementation Issues . . . 121
3.2.7 Residual Evaluation - Fault Detection . . . 122
3.2.8 Residual Evaluation - Fault Isolation . . . 122
3.2.8.1 Proposed Isolation Strategy . . . 123
3.2.9 Tuning of the FDI Scheme . . . 124
3.3 Simulation Results . . . 125
3.3.1 Residual Behaviour . . . 125
3.3.2 Monte Carlo Campaign . . . 126
3.3.3 Concluding Remarks on the Obtained FDI Results . . . 130
3.4 Recovery Aspects . . . 131
3.5 Conclusion . . . 132

4 Active FTC Approach for a New Thruster Configuration 137
4.1 New Thruster Configuration . . . 137
4.1.1 Feasibility of the Attainable Forces and Moments . . . 139
4.2 Context and motivations . . . 140
4.3 Robust Fault Detector Design . . . 140
4.3.1 Problem Setting . . . 141
4.3.2 Derivation of the Solution . . . 141
4.3.3 Residual Evaluation - Fault Detection . . . 144
4.4 Design of the Isolation Scheme . . . 145
4.4.1 Attitude Dynamics with Inertia Uncertainty . . . 145
4.4.2 Robust Nonlinear Unknown Input Observer Design . . . 148
4.4.3 Problem Statement . . . 149
4.4.4 LMI-based Synthesis . . . 150
4.4.5 Robustness Against Nonlinear Uncertainty . . . 152
4.4.6 NUIO Dynamics Adjustment . . . 153
4.4.7 Comments on NUIO Implementation and Computational Issues . . . 155
4.4.8 Thruster Group Isolation Logic - First Stage . . . 156
4.4.9 Final Thruster Fault Isolation - Second Stage . . . 157
4.5 Implementation and Tuning of the overall FDI Scheme . . . 159
4.6 Thruster Fault Accommodation . . . 160
4.6.1 Control Re-allocation . . . 161
4.6.2 Nonlinear Iterative Pseudoinverse Controller Approach . . . 162
4.6.3 Comparison of the NIPC Algorithm with the Existing Methods . . . 163
4.7 Simulation Results . . . 165
4.7.1 Illustrative Examples . . . 165
4.7.2 Monte Carlo Campaign . . . 167
4.8 Conclusion . . . 173

Conclusions and Perspective **175**

Appendices

A Mathematical Details **179**
A.1 Lemmas . . . 179
A.1.1 Neumann Series . . . 179
A.1.2 Millers's Lemma . . . 179
A.1.3 Schur's Complement . . . 180
A.1.4 Matrix Inequality Lemma . . . 180
A.2 Norms and Singular Values . . . 181
A.2.1 Vector Norms . . . 181
A.2.2 Matrix Norms . . . 181
A.2.3 Signal Norms . . . 182
A.2.4 Singular Values . . . 182
A.3 Pseudoinverses . . . 182
A.3.1 Moore-Penrose Pseudoinverse . . . 183
A.3.2 The Least Square Problem . . . 183
A.4 Cosine Direction Matrix for Attitude Modelling . . . 184
A.4.1 Definitions . . . 184
A.4.2 Basic Properties . . . 185
A.5 Quaternions . . . 185
A.5.1 Definition . . . 185
A.5.2 Conversion from Quaternion to Euler Angles . . . 186
A.5.3 Quaternion Product . . . 187

B Hypothesis Testing **189**
B.1 Wald's Sequential Probability Ratio Test . . . 189
B.1.1 Decision Test . . . 190
B.1.2 Calculation of the Decision Thresholds . . . 190
B.1.3 Wald's Test for the Mean Value . . . 192
B.1.3.1 Graphical Interpretation . . . 193
B.1.3.2 Modification to the Change of the Mean . . . 193
B.1.4 Wald's Test for the Variance . . . 194
B.1.4.1 Graphical Interpretation . . . 195
B.2 Generalized Likelihood Ration Test . . . 196
B.2.1 Decision Test . . . 196
B.2.1.1 GLR Test for the Mean Value . . . 196
B.2.1.2 GLR Test for the Variance . . . 197
B.2.2 On-line Realization . . . 198

References **199**

Index **219**

Colophon **221**

List of Figures

1 Distribution of AOCS component faults 2

1.1 General architecture of an active fault-tolerant control system 9
1.2 Open-loop system with different types of faults 11
1.3 The octahedron, dodecahedron and dedicated pyramid configuration 15
1.4 MEX spacecraft structure 19
1.5 Evolution of the conditional probability density 32
1.6 The HL-20 RLV vehicle 35
1.7 The H_∞ fault estimation problem 36
1.8 The FDI filter design problem 39
1.9 The quasi standard setup for the design of a robust fault detection filter 40
1.10 The generic structure of robust detection performance analysis problem 42
1.11 The Microscope satellite 43
1.12 Artist's concept of an HL-20 at a space station 44
1.13 LISA Pathfinder and its technology package 45
1.14 Adaptive threshold 46
1.15 Fault isolation 48
1.16 General structure of the UIO scheme 49
1.17 Control re-design approaches 51
1.18 Structured scheme of the multiple-model approach 51
1.19 Multiple model switching and tuning scheme 52
1.20 Bank of observers for sensor faults 54
1.21 Pseudo-inverse method 56
1.22 LQ-optimal control re-design 60
1.23 Fault-hiding paradigm scheme 62
1.24 The SLS optimization problem 65
1.25 Control allocation scheme 66
1.26 The structure of the supervisory FTC architecture 68

2.1 Illustration of the principal steps of the MSR mission 74
2.2 The chaser spacecraft, Mars ascent vehicle and the sample container 75
2.3 Mars rendezvous orbit 75
2.4 General setup of the chaser's GNC system during the rendezvous 76
2.5 The Mars rendezvous orbit with the associated frames 80
2.6 The phase plane profiles for the final approach: Y plane (left) and X plane (right) 80

2.7 The translation profiles and the attitude profile of the guidance loop 82
2.8 GNC of the chaser spacecraft 83
2.9 Geometrical interpretation of zeroing the off-diagonal elements of A_ϵ. 84
2.10 Robustness margins and performances of the attitude control loop 89
2.11 Robustness margins and performances of the position control loop 89
2.12 Control law (left) and the propulsion system (right) of the chaser vehicle 89
2.13 Scaled ON-times versus real thruster firing durations 90
2.14 Failure management unit with the location of the failure detection units 91
2.15 Sensor drift in the 1st accelerometer and performance degradation of the 2nd gyro 95
2.16 Sensor drift in the STR (left) and the corresponding quaternion (right) 96
2.17 The corridor shape during the rendezvous approach 97
2.18 Chaser attitude target pointing mode 101

3.1 "Half satellite" strategy for thruster faults 106
3.2 Baseline MSR thruster configuration of the chaser spacecraft 107
3.3 Torque directions (left) and force directions (right) 108
3.4 Set of attainable moments and forces 108
3.5 Position model-based FDI scheme 112
3.6 Attitude model-based FDI scheme 112
3.7 GLR signals based on a set of 200 Monte Carlo simulations 125
3.8 Residual behaviour for different scenarios 126
3.9 Behaviour of the internal signals of the position and attitude model-based FDI . 128
3.10 Behaviour of the internal signals of the position and attitude model-based FDI . 129
3.11 Histograms for thruster indices distribution and detection delays 130
3.12 Histograms for isolation and pure isolation delays 131
3.13 Capture position requirements and GNC performances for fault Case 1 132
3.14 Capture position requirements and GNC performances for fault Case 2 133
3.15 Capture angular requirements for fault Case 1 and Case 2 133
3.16 Capture position requirements and GNC performances for fault Case 3 133
3.17 Capture position requirements and GNC performances for fault Case 4 134
3.18 Capture angular requirements for fault Case 3 and Case 4 134

4.1 Thruster configuration of the chaser spacecraft 138
4.2 Torque directions (left) and force directions (right) 139
4.3 Set of attainable moments and forces 139
4.4 LMI Region $\mathcal{D}(\alpha, q, r, \beta) = \mathcal{D}_1 \cap \mathcal{D}_2 \cap \mathcal{D}_3$ 154
4.5 The overall structure of the proposed FDI scheme 159
4.6 FDI-based fault accommodation strategy implemented within the GNC architecture 161
4.7 Comparison of the NIPC approach with 7 other CA algorithms 164
4.8 Chaser trajectory within the MSR rendezvous corridor 165
4.9 Fault detection algorithm and NUIOs' dynamics behaviour for "open-type" fault 166
4.10 The overall isolation logic behaviour for "open-type" fault 167
4.11 Fault detection algorithm and NUIOs' dynamics behaviour for "closed-type" fault 167
4.12 The overall isolation logic behaviour for "closed-type" fault 168
4.13 Capture position requirements and GNC performances for fault the Case 1 . . . 170
4.14 Considered distributions and capture angular requirements for fault the Case 1 . 170
4.15 Capture position requirements and GNC performances for fault the Case 2 . . . 171
4.16 Considered distributions and capture angular requirements for fault the Case 2 . 171

4.17 Capture position requirements and GNC performances for fault the Case 3 . . . 172
4.18 Considered distributions and capture angular requirements for fault the Case 3 . 172

A.1 Definition of the orientation of the spacecraft axes in the reference frame 184

B.1 Definition of the probability of non-detection and false alarm 190
B.2 Graphical interpretation of the Wald's decision test for the mean value 194
B.3 Graphical interpretation of the Wald's decision test for the variance 195

List of Tables

1 List of on-orbit thruster failures 3

1.1 Classification of the introduced AFTC approaches 71
1.2 Classification of the existing FDI approaches 72

2.1 MSR conditions for successful capture 75
2.2 Keplerian orbital parameters (initial) of the chaser and target 76
2.3 Considered parameter uncertainties of the chaser spacecraft 88
2.4 Hierarchical fault detection levels 92

3.1 Evaluated FDI performance indices based on 4x1600 Monte Carlo runs 129

4.1 Comparison of the CA algorithms in terms of computational burden 164
4.2 FDI performances based on 3×1000 Monte Carlo runs 169

B.1 Decision situations in a two-hypothesis test 189

Nomenclature

In general, symbols are used according to the following conventions: scalars are represented by italics like $\{a, b, c\}$; vectors by bold-italic lowercase letters like $\{\boldsymbol{u}, \boldsymbol{x}, \boldsymbol{y}\}$; matrices by bold-italic capital letters like $\{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}\}$; and sets are denoted by calligraphic letters like $\{\mathcal{D}, \mathcal{G}, \mathcal{S}\}$. For the sake of notation simplicity, the time dependence of signals is sometimes omitted when there are no confusions.

Symbols and Variables

a	[scalar]	radius of the target's circular orbit (m)
$\boldsymbol{b}$	$[3 \times 1]$	vector of sensor biases (deg/s)
$\bar{\boldsymbol{B}}$	$[6 \times N]$	overall thruster configuration matrix
$\boldsymbol{d}_k$	$[3 \times 1]$	unit vector indicating the thrust direction of the kth thruster
$\boldsymbol{d}_{p_k}$	$[3 \times 1]$	position (location) vector of the kth thruster w.r.t. $\mathcal{F}_b$ (m)
$\boldsymbol{d}_{CoM}$	$[3 \times 1]$	position (location) vector of the center of mass w.r.t. $\mathcal{F}_b$ (m)
$\boldsymbol{d}$	$[n_d \times 1]$	disturbance (unknown input) vector
$\boldsymbol{f}$	$[n_f \times 1]$	additive fault vector
$\boldsymbol{F}$	$[3 \times 1]$	force vector (N)
$\boldsymbol{F}_d$	$[3 \times 1]$	vector of commanded forces (N)
$\boldsymbol{I}, (\boldsymbol{0})$	[suitable]	identity (zero) matrix with appropriate dimensions
$\boldsymbol{J}$	$[3 \times 3]$	inertia matrix (kg·m^2)
$\boldsymbol{L}$	$[n_x \times n_y]$	observer gain matrix
m_c	[scalar]	mass of the chaser spacecraft (kg)
$\hat{m}_{loss}$	[scalar]	thrust loss size
$\hat{m}_{leak}$	[scalar]	maximum leakage size
m_M	[scalar]	mass of the Mars planet (kg)
n	[scalar]	uniform orbital rate of the target target (N.m^2.kg^{-1})
$\boldsymbol{q}_t$	$[4 \times 1]$	quaternion describing the orientation of the target w.r.t. $\mathcal{F}_i$
$\boldsymbol{q}_c$	$[4 \times 1]$	quaternion describing the orientation of the chaser w.r.t. $\mathcal{F}_i$
$\boldsymbol{r}$	$[n_r \times 1]$	vector of residual signal
T	[scalar]	sampling interval (s)
$\boldsymbol{T}$	$[3 \times 1]$	torque vector (N.m)
$\boldsymbol{T}_d$	$[3 \times 1]$	vector of commanded torques (N.m)
$\boldsymbol{u}$	$[n_u \times 1]$	general system input vector

$\tilde{\boldsymbol{u}}$	$[N \times 1]$	vector of scaled thruster open durations
$\boldsymbol{u}_c$	$[3 \times 1]$	controlled system input vector
$\boldsymbol{x}$	$[n_x \times 1]$	state vector
$\boldsymbol{z}$	$[n_z \times 1]$	augmented state vector
$\boldsymbol{y}$	$[n_y \times 1]$	output vector
κ	[scalar]	design parameter ($\mathcal{L}_2$ attenuation) for the NUIO
ϵ	[scalar]	some tolerance close to zero
ν	[scalar]	true anomaly (rad)
$\mathcal{G}$	[scalar]	universal gravitational constant (N.m^2.kg^{-2})
$\tau(t)$	[scalar]	time-varying delay (s)
ξ, η, ζ	[scalars]	Cartesian component of the relative position (m)
φ, θ, ψ	[scalars]	roll, pitch, and yaw angle (deg)
p, q, r	[scalars]	roll, pitch, and yaw rate (deg·s^{-1})
$\boldsymbol{\Psi}$	$[N \times N]$	multiplicative fault-modelling matrix

Dimensions

n_x	length of the state vector
n_u	length of the input vector
n_y	length of the output vector
n_r	residual signal dimension
n_{mc}	number of Monte Carlo runs
N	number of thrusters (8 or 12)

Superscripts

$\bullet^T$	matrix or vector transpose
$\hat{\bullet}$	an estimated value
$\vec{\bullet}$	vector in cartesian form

Subscripts

$_a$	attitude model
$_p$	position model
$_f$	faulty case

Reference frames

$\mathcal{F}_b$	body, chaser's center of mass-fixed frame
$\mathcal{F}_l$	local, target-fixed frame
$\mathcal{F}_i$	inertial, Mars-centered frame

Sets

$\mathcal{D}$	set defining an LMI region
$\mathcal{S}_{all}$	set of all thruster indices
$\mathcal{S}_{Tk}$	set (group) of thrusters with similar properties
$\mathbb{R}, \mathbb{C}$	set of real and complex numbers
$\mathbb{Z}^+$	set of non-negative integers
$\mathbb{H}$	set of quaternions
$\mathcal{C}$	compact set

Times

t	general notation for a continuous time
t_f	fault occurrence time
$t_d, (\tau_d)$	fault detection time (delay)
$t_i, (\tau_i)$	fault isolation time (delay)
$t_g, (\tau_g)$	fault group isolation time (delay)
k	discrete time instance $t_k = kT$

Math Notation

$\boldsymbol{A}^\dagger$	Moore–Penrose pseudoinverse of $\boldsymbol{A}$
diag(...)	block diagonal matrix
Im/Ker	image/kernel of a linear transformation (matrix)
dim	dimension of a vector space
rank($\boldsymbol{A}$)	rank of a matrix $\boldsymbol{A}$
sign(x)	signum function of a real number x
$\otimes, \odot$	Kronecker, quaternion product
$[\cdot, \cdot]$	Lie's bracket of two elements
$\boldsymbol{P} > 0$ ($\boldsymbol{P} < 0$)	means that $\boldsymbol{P}$ is a real symmetric and positive (negative) definite matrix
$\Lambda(\boldsymbol{A})$	set of all the eigenvalues of a square matrix $\boldsymbol{A}$
" $*$ "	element induced by symmetry in a symmetric block matrix
$\lVert \cdot \rVert$	2-norm of a vector or the induced matrix 2-norm
$\lVert \cdot \rVert_F$	Frobenius norm of a matrix
$\lVert \cdot \rVert_{lp}$	$\mathcal{L}_p$-norm of a signal, $p \in \{1, 2, \infty\}$
$\lvert \cdot \rvert$	absolute value of ascalar
$\mathcal{L}_p$	space of all $\mathcal{L}$ebensque measurable functions having a finite $\mathcal{L}_p$ norm
$\{\ldots\}$	set
$E\{\cdot\}$	expectation
$\boldsymbol{a} \cdot \boldsymbol{b}$	dot (scalar) product of vectors $\boldsymbol{a}$ and $\boldsymbol{b}$
$\boldsymbol{a} \times \boldsymbol{b}$	cross (vector) product of vectors $\boldsymbol{a}$ and $\boldsymbol{b}$
δ_{ij}	Kronecker's delta
$\mathcal{U}(a, b)$	is the uniform distribution with boundaries a and b
$\mathcal{N}(\mu, \sigma^2)$	normal (Gaussian) distribution with mean value μ and variance σ^2

Abbreviations

AFTCS Active-Fault Tolerant Control System

AMM Autonomous Mission Management

AOCS Attitude and Orbit Control System

ATV Automated Transfer Vehicle

CA Control Allocation

CDF Cumulative Distribution Function

CGI Cascading Generalized Inverse

CNES Centre National d'Études Spatiales (National Centre for Space Studies)

CNRS Centre National de la Recherche Scientifique (French National Centre for Scientific Research)

CPDE Chemical Propulsion Drive Electronics

CRAN Centre de Recherche en Automatique de Nancy (Research Centre for Automatic Control of Nancy)

CSS Coarse Sun Sensors

DIR Direct Control Allocatio

DOF Degree of Freedom

DTU Danmarks Tekniske Universitet (Technical University of Denmark)

EA Eigenstructure Assignment

EKF Extended Kalman Filter

EMF Explicit Model Following

ESA European Space Agency

ESTEC European Space Research and Technology Centre

FD Fault Detector

FDD Fault Detection and Diagnosis

FDI Fault Detection and Isolation

FDIR Fault/Failure Detection, Isolation and Recovery

FEEP Field Emission Electric Propulsion

FMEA Fault Mode and Effect Analysis

FTC Fault-Tolerant Control

FXP Fixed-Point

GLR Generalised Likelihood Ratio

GNC Guidance Navigation Control

GNSS Global Navigation Satellite System

HCW Hill–Clohessy–Wiltshire

IFAC International Federation of Automatic Control

ILO Iterative Learning Observer

IMM Interacting Multiple Models

IMS Intégration du Matériau au Système (Material and System Integration)

IMU Inertial Measurement Units

IP Inerior Point

ISS International Space Station

LFR Linear Fractional Representations

LIDAR Light Detection and Ranging

LISA Laser Interferometer Space Antenna

LMI Linear Matrix Inequalities

LPV Linear Parameter-Varying

LQ Linear Quadratic

LTI Linear Time-Invariant

LTV Linear Time-Varying

MAV Mars Ascent Vehicle

MC Monte Carlo

MEX Mars Express

MIB Minimum Impulse Bit

MIMO Multiple Input Multiple Output

MLS Minimal Least-Squares

MM Multiple Model

MMST Multiple Model Switching and Tuning

MPC Model Predictive Control

MSR Mars Sample Return

NAC Narrow Angle Camera

NASA National Aeronautics and Space Administration

NAV Navigation Unit

NIPC Nonlinear Iterative Pseudoinverse Controller

NPI Networking/Partnering Initiative

NUIO Nonlinear Unknown Input Observer

PDF Probability Density Function

PFTCS Passive-Fault Tolerant Control System

PIM Pseudo-Inverse Method

QCAT Quadratic Programming Control Allocation Toolbox

RFS Radio Frequency Sensor

RLV Re-entry Launched Vehicle

SACM Sun Acquisition Mode

SHM System Health Management

SHS Sample Handling System

SISO Single Input Single Output

SLS Sequential Least-Square

SMO Sliding Mode Observer

SPRT Sequential Probability Ration Test

STR Star Tracker

SZTAKI Számítástechnikai és Automatizálási Kutatóintézet (Institute for Computer Science and Control)

TAS Thales Alenia Space

TLV Thruster Latch Valve

TMF Thruster Management Function

TMU Thruster Modulator Unit

UAV Unmanned Aerial Vehicle

UIO Unknown Input Observer

UKF Unscented Kalman Filter

WLS Weighted Least-Squares

Terminology

The terminology used in this thesis is in accordance with the International Federation of Automatic Control (IFAC) Safeprocess Technical Committee terminology in the field of fault diagnosis and fault-tolerant control as listed below. These definitions can also be found in [18, 19, 146, 147]

Active fault-tolerant system: a fault-tolerant system where faults are explicitly detected and accommodated. Opposite of a passive fault-tolerant system.

Analytical redundancy: use of two or more (but not necessarily identical) ways to determine a variable, where one way uses a mathematical process model in analytical form.

Availability: likelihood that a system or equipment will operate satisfactorily and effectively at any point of time.

Autonomy: The ability for a spacecraft and its on-board systems to perform a function without external support.

Dependability: a form of availability that has the property of always being available when required.

Constraint: the limitation imposed by nature (physical law) or man. It permits the variables to take only certain values in the variable space.

Controlled system: a physical plant under consideration with sensors and actuators used for control.

Decision logic/rule: the functionality that decides what type of corrective action(s) to execute in case of a reported fault and which alarm(s) shall be generated.

Disturbance: an unknown (and uncontrolled) input acting on a system.

Error: a deviation between a measured or computed value (of an output variable) and the true, specified or theoretically correct value.

Failure: a permanent interruption of a system's ability to perform a required function under specified operating conditions.

Fault: an unpermitted deviation of at least one characteristic property or parameter of the system from the acceptable (usual) standard condition.

Fault accommodation: an adequate change of the control law in order to avoid the consequences of a fault. The input-output relations (channels) between the controller and plant are unchanged. The original control objective is achieved although performance may degrade.

Fault detection: determination of the faults present in a system and the time of detection.

Fault detector: an algorithm that performs fault detection and eventually also fault isolation.

Fault diagnosis: determination of the kind, size, location and time of detection of a fault. It follows fault detection. It includes the fault isolation and identification (estimation).

Fault identification: determination of the size and time-variant behavior of a fault. Follows fault isolation. Used as a synonym for "fault estimation".

Fault isolation: determination of the kind, location and time of detection of a fault. Follows fault detection.

Fault modelling: determination of a mathematical model to describe a specific fault effect.

Fault recovery: the result of a successful fault accommodation or a system reconfiguration.

Fault tolerance: the ability of a controlled system to maintain control objectives, despite the occurrence of a fault. A degradation of the control performance may be accepted. Fault-tolerance can be obtained through fault accommodation or through system and/or controller reconfiguration.

Hardware redundancy: use of more than one independent instrument to accomplish a given function.

Incipient fault: a fault where the effect develops slowly (e.g., clogging of a valve). It is in opposite to an abrupt fault.

Model: a mathematical representation of a physical system or process intended to enhance the ability to understand, predict or control its behavior.

Monitoring: a continuous real-time task of determining the conditions of a physical system, by recording information, recognizing and indicating anomalies in the behavior.

Passive fault-tolerant control system: a fault-tolerant system where faults are not explicitly detected and accommodated, but the controller is designed to be insensitive to a certain restricted set of faults. It is in contrary to an active fault-tolerant system.

Perturbation: an input acting on a system, which results in a temporary departure from the current state.

Qualitative model: model using static and dynamic relations among system variables and parameters in order to describe a system's behavior in qualitative terms such as causalities or if-then rules.

Quantitative model: model using static and dynamic relations among system variables and parameters in order to describe a system behavior in quantitative mathematical terms such as differential or difference equations.

Reliability: probability of a system to perform a required function under normal conditions and during a given period of time.

Residual: signal containing information about fault(s), based on a deviation between measurements and model based computations.

Residual generation: is a procedure of extracting fault symptoms from the system, using the available input/output information.

Residual evaluation: the process of comparing residuals to some predefined thresholds, directions or evaluation function. This is a stage where symptoms are produced.

Residual generator: is an computational algorithm used to generate residuals.

Safety: ability of a system not to cause danger to persons or equipment or the environment.

System reconfiguration: change in input-output between the controller and the plant through change of the controller structure and parameters. The original control objective is achieved although performance may degrade.

Supervision: monitoring a physical system and taking appropriate actions to maintain the operation in case of faults.

Symptom: a change of an observable quantity from normal behavior.

Threshold: limit value of a residual's deviation from zero, so if exceeded, a fault is declared as detected.

List of Publications of the Author

Publications Related to the Thesis

[1] **Fonod, R.**, Henry, D., Charbonnel, C., Bornschlegl, E., Losa, D., and Bennani, S. "Active FTC Approach for Thruster Faults: Application to a Deep Space Mission." Preprint submitted to: *Control Engineering Practice*, **CEP**, November 2014.

[2] **Fonod, R.**, Henry, D., Charbonnel, C., and Bornschlegl, E. "Position and Attitude Model-Based Thruster Fault Diagnosis: A Comparison Study", *AIAA Journal of Guidance, Control and Dynamics*, **JGCD**, accepted for publication, doi: 10.2514/1.G000309, September 2014.

[3] **Fonod, R.**, Henry, D., Bornschlegl, E., and Charbonnel, C. "Thruster Fault Detection, Isolation and Accommodation for an Autonomous Spacecraft." In *Proc. of the 19th IFAC World Congress*, **IFAC WC'14** *(invited session)*, Cape Town, South Africa, August 2014.

[4] **Fonod, R.**, Henry, D., Charbonnel, C., and Bornschlegl, E. "A Class of Nonlinear Unknown Input Observer for Fault Diagnosis: Application to fault tolerant control of an autonomous spacecraft." In *Proc. of the 10th UKACC International Conference on Control*, **CONTROL'14**, Loughborough, United Kingdom, July 2014. (winner of the **Best Student Submission Award**)

[5] **Fonod, R.**, Henry, D., Bornschlegl, E., and Charbonnel, C. "Robust Fault Detection for Systems with Electronic Induced Delays: Application to the rendezvous phase of the MSR mission." In *Proc. of the 12th European Control Conference*, **ECC'13**, Zürich, Switzerland, July 2013.

[6] **Fonod, R.**, Henry, D., Charbonnel, C., and Bornschlegl, E. "Robust Thruster Fault Diagnosis: Application to the rendezvous phase of the Mars Sample Return mission." In *Proc. of the 2nd CEAS Specialist Conference on Guidance, Navigation and Control*, **EuroGNC'13**, Delft, Netherlands, April 2013.

[7] **Fonod, R.**, Henry, D., Bornschlegl, E., and Charbonnel, C. "Robust Fault Diagnosis for Systems with Electronic Induced Delays." In *Proc. of the 10th European Workshop on Advanced Control and Diagnosis*, **ACD'12**, Copenhagen, Denmark, November 2012.

Other Publications

[8] **Fonod, R.**, and Krokavec, D. "Actuator Fault Estimation Using Neuro-sliding Mode Observers." In *Proc. of the 16th IEEE International Conference on Intelligent Engineering Systems*, **INES'12**, Lisbon, Portugal, June 2012.

[9] Gontkovic, D., and **Fonod, R.** "State Control Design for Linear Systems with Distributed Time Delays." In *Proc. of the 10th IEEE International Symposium on Applied Machine Intelligence and Informatics*, **SAMI'12**, Herlany, Slovakia, January 2012.

[10] Gontkovic, D., and **Fonod, R.** "Control and Stability Analyzing of the Time-delay Systems with Time-varying Delays", *Acta Electrotechnica et Informatica*, **AEI**, Vol. 11, No.3, pp. 70–74, 2011.

[11] Kocsis, P., and **Fonod, R.** "Eigenstructure Decoupling in State Feedback Control Design", *A&TP Journal plus*, **ATP**, No. 2, pp. 34–39, 2011.

[12] **Fonod, R.**, and Kocsis, P. "State Feedback Control Design Using Eigenstructure Decoupling." In *Proc. of the 18th International Conference on Process Control*, **PC'11**, Tatranska Lomnica, Slovakia, June 2011.

[13] **Fonod, R.**, and Gontkovic, D. "Fault Estimation in a Class of First Order Nonlinear Systems." In *Proc. of the 9th IEEE International Symposium on Applied Machine Intelligence and Informatics*, **SAMI'11**, Smolenice, Slovakia, January 2011.

Résumé en Français

Les travaux de recherche traités dans cette thèse s'appuient sur l'expertise des actions menées entre l'Agence spatiale européenne (ESA), l'industrie française Thales Alenia Space (TAS) et le laboratoire de l'Intégration du matériau au système (IMS) qui vise à développer de nouvelles générations d'unités intégrées de guidage, navigation et pilotage (GNC) avec une fonction de détection des défauts et de tolérance des défauts.

Beaucoup de futures missions spatiales requerront des opérations de proximité autonomes dans lesquelles la détection des défauts, la localisation et les mesures de tolérance des défauts qui en découlent, sont d'une importance cruciale. Les missions de rendez-vous et d'amarrage/capture, comme pour la mission Mars Sample Return (MSR) et le Project for On-Board Autonomy No.3 (PROBA 3) sont aussi intrinsèquement liés aux conditions de fonctionnement et à la sécurité des engins spatiaux. Les rendez-vous autonomes et les tolérances de défauts ont été reconnus par l'ESA comme un élément clé des futures missions dans l'espace lointain, ce qui nécessitera un système GNC hautement sophistiqué.

Cette thèse porte sur la conception et la validation d'un système de commande à tolérance de défaut actif pour détecter, isoler et s'adapter à un défaut de tuyère qui affecte un vaisseau spatial chasseur lors d'un rendez-vous avec un vaisseau spatial cible passif sur une orbite circulaire. La mission de référence retenue dans cette thèse est la mission MSR de l'ESA. La mission MSR se compose de deux modules (engins spatiaux) injectés directement vers Mars par des lanceurs. Le premier module pénètre dans l'atmosphère martienne (phase d'entrée), atterrit sur la surface de Mars et libère un véhicule astromobile sur Mars. Une fois que le véhicule astromobile termine la procédure de collecte des échantillons martiens, ces derniers sont ensuite placés dans un conteneur d'échantillons et chargés sur un véhicule de montée sur Mars (MAV) qui est ensuite lancé, au moyen de fusées, pour atteindre l'orbite basse de Mars. Entretemps, le second module, composé de l'orbiteur MSR et de la capsule de rentrée sur Terre (ERC), s'insère directement autour de Mars, et le véhicule chasseur attrape la cible (capture des échantillons en orbite libéré par MAV), et enfin revient sur Terre éjecter les échantillons dans l'atmosphère de la Terre avec la capsule de rentrée sur Terre (ERC). La problématique abordée dans cette thèse se concentre sur la séquence terminale du rendez-vous de la mission MSR qui correspond aux dernières centaines de mètres jusqu'à la capture.

Le véhicule chasseur est l'orbiteur MSR (chasseur), alors que la cible passive est un conteneur sphérique. Pendant le rendez-vous terminal, le contrôle de l'attitude et la position du chasseur est continue, et rectifié par les tuyères. L'attitude est contrôlée afin de maintenir le conteneur d'échantillon (cible) dans le champ de vue du capteur LIDAR (Light Detection and Ranging).

La position est contrôlée afin de se rapprocher de l'objectif le long de son axe de vitesse. Ensuite, juste avant la capture, le guidage est modifié afin d'aligner le mécanisme de capture avec la cible. Au niveau du capteur, le vaisseau spatial chasseur utilise un IMU (Inertial Measurement Units) et un viseur d'étoiles (DOS) pour le contrôle d'attitude et d'un LIDAR pour le contrôle de position et de capture. L'ensemble des capteurs et des vérins pendant le rendez-vous terminal est minimisé pour réduire le risque de défaillance et pour réduire la masse et la consommation d'énergie. Les conditions de capture sont commandées par le mécanisme de capture. Le mécanisme de capture est un panier avec une ouverture cylindrique qui fait partie du système de manipulation d'échantillons (SHS). Il est orienté selon l'axe des x de l'orbiteur et situé avec un décalage latéral sur la face +x. L'objectif au niveau de contrôle est de réaliser la capture avec une précision inférieure à quelques centimètres.

La phase terminale du rendez-vous est très critique, car toute défaillance pourrait éventuellement conduire à une collision, et à un échec de la mission. Il est évident, que si, par exemple, une défaillance ouvrant entièrement une tuyère se produit (une tuyère coincée en position entièrement ouverte), elle pourrait conduire à une augmentation drastique de la consommation de gaz du propulseur qui est déjà très limitée par le voyage vers Mars. En outre, des conséquences dramatiques peuvent survenir, par exemple le système classique GNC peut entraîner une performance peu satisfaisante et/ou une instabilité, pouvant conduire le chasseur à perdre l'attitude et/ou la position du conteneur d'échantillons. Le problème devient particulièrement critique au cours des 20 derniers mètres de la phase de rendez-vous. Des études récentes ont montré qu'historiquement les défauts de tuyère représentent approximativement un quart de toutes les défaillances qui ont eu lieu en orbite.

Une détection rapide et une localisation de ces défaillances est la première étape vers une action efficace de correction du défaut. L'utilisation de capteurs de pression et de température spécialisées dans la tuyère d'un propulseur est une possibilité de détecter une défaillance de propulseur. Ceci, cependant, entraine une hausse de la masse, du prix et de la complexité. Cette thèse se concentre donc plutôt sur des solutions basées uniquement sur des logiciels supplémentaires et du matériel déjà disponible à bord. Les travaux de recherche traités dans cette thèse s'intéressent donc au développement des approches sur base de modèle de détection et d'isolation des défauts (Fault Detection and Isolation, FDI) et de commande tolérante aux défaillances (Fault Tolerant Control, FTC), qui pourraient augmenter d'une manière significative l'autonomie opérationnelle et fonctionnelle du chasseur pendant le rendez-vous et, d'une manière plus générale, d'un vaisseau spatial impliqué dans des missions situées dans l'espace lointain. Dès lors que la redondance existe dans les capteurs et que les roues de réaction ne sont pas utilisées durant la phase de rendez-vous, le travail présenté dans cette thèse est orienté seulement vers les systèmes de propulsion par tuyères.

Les défaillances examinées ont été définies conformément aux exigences de l'ESA et de TAS et suivant leurs expériences. Quatre cas sont étudiés en détail, à savoir: i) ouverture de tuyère à 100%, dans ce cas, la tuyère fournit une poussée maximale indépendamment de la demande et est évidemment très consommatrice de propergol; ii) tuyère coincée en position fermée, dans ce cas la tuyère défectueuse ne génère aucune poussée indépendamment de la commande faite par l'autorité de contrôle; iii) une petite fuite de biergol et iv) une perte d'efficacité d'une tuyère spécifique, à savoir la poussée réelle est inférieure à celle qui est demandée.

Cette thèse comprend un chapitre qui illustre certains concepts, définitions et résultats classiques ainsi que quelques exemples de mise en œuvre réussie des approches de l'FDI et de la FTC dans

certaines missions spatiales. On aborde ensuite, une description complète du système GNC déjà en place ainsi que la gestion de panne. Dans les études menées dans cette thèse, deux configurations de propulseurs différentes ont été étudiées. La première configuration (référence) dispose d'un ensemble de propulseur entièrement redondant de 2x8 tuyères tandis que la seconde configuration comprend 12 tuyères avec redondance fonctionnelle.

Pour la première configuration des tuyères (référence) une approche avancée détection/ défaillance, isolation de défauts et reconfiguration (FDIR) est proposée. Elle se compose d'un détecteur de défaut robuste et d'un test d'isolement en fonction d'une corrélation croisée. La reconfiguration des défauts est réalisée par une simple redirection du signal vers la tuyère redondante et la fermeture de la tuyère défectueuse par une soupape de verrouillage de la tuyère (TLV). Le détecteur de défaut est basé sur un générateur résiduel avec robustesse accrue contre le retard de variation de temps inconnue dans le canal d'entrée. Ce retard est induit par le dispositif électronique de guidage de la propulsion chimique (CPDE) et vise également à modéliser les incertitudes sur les temps de réponse de la tuyère. Pour assurer la robustesse, l'incertitude non structurée (effet du retard inconnu) est d'abord exprimée sous forme d'une entrée inconnue, puis, cette entrée inconnue est découplée du résidu en utilisant la technique de Eigenstructure Assignment (EA) à gauche. Deux méthodes pour transformer ce type d'incertitude en une entrée inconnue sont proposées. La première méthode est basée sur le théorème de Cayley-Hamilton et sur un h-ième ordre de l'expansion en série de Taylor ; le second procédé utilise dans un premier ordre l'approximant de Padé du retard temporel variable dans le temps.

Les indices de performance et de fiabilité FDI, qui ont été soigneusement choisis, accompagnés des campagnes de simulation de robustesse/sensibilité Monte Carlo (MC) ont été utilisés pour l'étude de comparaison des deux schémas FDI, l'une basée sur une position et la seconde basée sur un modèle d'attitude. Les aspects de la reconfiguration sont également étudiés. Les résultats obtenus à partir de la campagne MC, effectuée à l'aide d'un simulateur industrielle haute-fidélité du TAS, révèlent que le régime basé sur un modèle de position tend à atteindre une performance très similaire à celle du régime fondé sur le modèle de l'attitude pure. Le schéma du modèle basé sur la position réussi grâce au modèle linéaire judicieusement choisi, c'est à dire un modèle qui prend en compte à la fois les mouvements de rotation et de translation du chasseur. Dans ce modèle, le quaternion d'attitude joue le rôle de paramètre d'ordonnancement pour la génération de résidus. De plus ce modèle est naturellement robuste contre les incertitudes sur l'inertie et le centre de gravité.

Pour une autre configuration de propulseur qui a été spécialement développé par Thales Alenia Space pour étudier les principes FTC actifs, un schéma innovant FDI/FTC est proposé pour isoler sans ambiguïté et s'adapter à tout type de défaillance de tuyère (de types ouvert ou fermé) affectant le système de propulsion du chasseur. Cette configuration diffère de la configuration de base de la mission MSR car les propulseurs n'ont pas de pair redondante et certains propulseurs génèrent un moment de torsion dans la même direction ou dans une direction très similaire, ce qui rend évidemment le procédé d'isolement plus difficile. Le schéma FDI consiste en un détecteur de défaut robuste qui déclenche une banque d'observateur non linéaire à entrées inconnues (NUIOs) qui est en charge de confiner la défaillance à un sous-ensemble de défauts possibles, et une logique d'isolement à deux niveaux qui correspond respectivement au moment de torsion d'un propulseur fixe et des directions de force avec le biais de moment de torsion (estimé en utilisant un filtre de Kalman étendu, EKF) et du signal résiduel du détecteur de défaut. La principale caractéristique de ce schéma FDI est le développement d'une classe spéciale de NUIO pour les dynamiques d'attitude non linéaires incertaines. Sous certaines hypothèses de Lipschitz,

une contrainte d'atténuation $\mathcal{L}2$ est envisagée pour minimiser l'effet de l'inertie incertaine sur l'erreur d'estimation de l'état. La factorisation proposée de l'inversion de la matrice d'inertie incertaine permet à la dynamique de l'observateur à être limitée dans une région dynamique prévue tandis qu'est maximisée la constante de Lipschitz acceptable entrainant la robustesse contre les incertitudes non linéaires de Lipschitz. En outre, la dynamique d'erreur d'estimation est exactement découplée de l'entrée inconnue qui représente l'effet du groupe de propulseur qui produit les mêmes moments de torsion ou des moments de torsion similaires. La synthèse NUIO est formulée comme un problème d'optimisation convexe d'inégalité matricielle linéaire (LMI). La tolérance de défaillance est atteinte par la fermeture du propulseur défectueux par une soupape de verrouillage et en redistribuant les forces/moment de torsion souhaités parmi les N-1 vérins sains utilisant un algorithme d'allocation de contrôle (CA). L'avantage de cette approche est la réduction du nombre de propulseurs (pas d'ensemble redondant) nécessaires pour contrôler l'engin spatial en toute sécurité qui crée par conséquent un gain de masse, de volume et de complexité. Plusieurs techniques de CA sont évaluées pour leur pertinence à atteindre la tolérance aux défaillances précitée. La technique de CA NIPC (Nonlinear Iterative Pseudoinverse Controller) a été choisie et améliorée à des fins FTC.

Les résultats obtenus à partir de la campagne de simulation MC, effectués à l'aide d'un simulateur industrielle haute-fidélité du TAS, mettent en évidence la pertinence des approches FDI/FTC proposées. L'évaluation des critères orientés de mission démontre clairement que la stratégie à tolérance de défaut proposée est en mesure de faire face à une grande catégorie de défauts de tuyères malgré la présence de différents types d'incertitudes et de garantir le succès de la capture. En d'autres termes, les schémas FDI/FTC proposées sont capables de détecter, d'isoler et de s'adapter à tous les types de défaut de tuyères considérés qui pourraient mettre en danger la réussite de la mission. Il est également montré que les petits défauts de propulseurs, comme les petites pertes de poussée (qui sont très difficiles, voire impossibles à détecter et isoler), ont des effets négligeables sur le maintien de la performance GNC (par exemple en termes de précision de pointage) et/ou sur les exigences finales de capture MSR.

Pour conclure, tous les résultats obtenus dans cette thèse ont révélé que les deux techniques FDIR avancé et FTC ont de grands avantages en termes de fiabilité, de sécurité et de succès de la mission par rapport aux approches classiques FDIR (industriels). Grâce à la bonne connaissance des sous-systèmes qu'ont les ingénieurs de l'ESA et de TAS, le FMEA (Fault Mode and Effect Analysis) rend plus facile le développement d'un schéma spécifiques FDI/FTC dédiés à certains sous-ensemble de défauts survenant dans un vrai vaisseau spatial. C'est une des nombreuses raisons pour lesquelles les précieuses connaissances des ingénieurs de systèmes de contrôle ayant collaboré au sein de ce projet furent cruciales.

Introduction

"You don't write because you want to say something,
you write because you have something to say."
— F. Scott Fitzgerald, American writer

Focus of this Study

The research work addressed in this thesis draws expertise from actions undertaken between the European Space Agency (ESA), the industry Thales Alenia Space (TAS) and the IMS laboratory (laboratoire de l'Intégration du Matériau au Système) which aims at developing new generations of integrated Guidance, Navigation and Control (GNC) units with fault detection and tolerance capabilities. Many future space missions will require autonomous proximity operations, in which the fault detection, isolation and the subsequent fault tolerance actions are critically important. Rendezvous and docking/capture missions, such as the Mars Sample Return (MSR) mission and the Project for Onboard Autonomy No.3 (PROBA 3), are also inherently concerned with the fail-safe operating conditions of the vehicles. Autonomous and fault tolerant rendezvous has been recognized by ESA as a key element for the MSR mission, which will require a highly sophisticated GNC system. For instance, for a success of the critical rendezvous phase, the chaser vehicle uses a large range of sensors, namely Inertial Measurement Units (IMU), Star Trackers (STR), Coarse Sun Sensors (CSS), Global Navigation Satellite Systems (GNSS) sensors, Radio Frequency Sensors (RFS), Light Detection And Ranging (LIDAR) sensors, Narrow Angle Camera (NAC) and a very precise actuation system composed of sets of thrusters and reaction wheels. It is then obvious, that the rendezvous mission can be in danger if faults occur in these sensors and/or actuators and if the GNC system does not adequately compensate them. The research work addressed in this thesis draws expertise in this context.

More precisely, this thesis focuses on the design and validation of an active Fault-tolerant Control (FTC) system to detect, isolate and accommodate thruster fault affecting a chasing spacecraft during the rendezvous with a passive target spacecraft in a circular orbit. A FDIR (Fault/Failure Detection, Isolation and Recovery) system is also developed to be compliant with the requirements and the current state of practice of the space industries. The reference mission considered here is the ESA Mars Sample Return mission. It consists of two modules directly injected towards Mars by launchers. The first module enters the Martian atmosphere (Entry phase), lands

on the Mars surface and releases a Mars rover vehicle. Once the rover finishes the collection procedure of the Martian samples, they are put into a Sample Container and loaded on the Mars Ascent Vehicle (MAV) which is then launched, by means of rockets, to reach the low Mars orbit. Meanwhile the second module, composed of the MSR Orbiter and the Earth Re-entry Capsule (ERC), inserts directly around Mars, and the chaser vehicle catches the target (capture of the orbiting Sample Container released by MAV) and finally comes back to Earth ejecting the Sample Container into Earth atmosphere with the Earth Re-entry Capsule (ERC). The research work addressed in this thesis focuses on the terminal rendezvous phase which corresponds to the last meters until the capture. The chaser vehicle is the MSR Orbiter, while the target is a diameter spherical container. During the terminal rendezvous, the control of the attitude and the position of the chaser is continuous, and applied by thrusters. The attitude is controlled in order to keep the Sample Container (target) within the LIDAR sensor field of view. The position is controlled in order to approach the target along its velocity axis. Then, just before the capture, the guidance is modified in order to align the capture mechanism with the target. At sensor level, the chaser spacecraft uses IMUs and Star-Trackers for attitude control and a LIDAR for position control and capture. The set of sensors and actuators used during the terminal rendezvous is minimized to reduce the risk of fault occurrence and to reduce the power consumption and mass. The capture conditions are driven by the capture mechanism. The capture mechanism is a basket with a diameter cylindrical aperture, which is part of the Sample Handling System (SHS). It is oriented along the Orbiter x axis and located with a lateral offset on the +x face. The analysis is conducted in the context of the terminal rendezvous sequence. The objective at control level is a capture achievement with an accuracy better than a few centimeters.

Motivation

The terminal phase of the rendezvous is highly critical, as any fault could possibly lead to a collision, thus to a mission loss. Thruster faults historically account for a largest percentage of failures that have occurred on orbit. Following a recent and extensive study based on 129 military and commercial spacecrafts from 1980 to 2005, thruster faults account for approximatively one quarter of all Attitude and Orbit Control System (AOCS) failures [272], see Fig. 1 showing the distribution of various AOCS component failures.

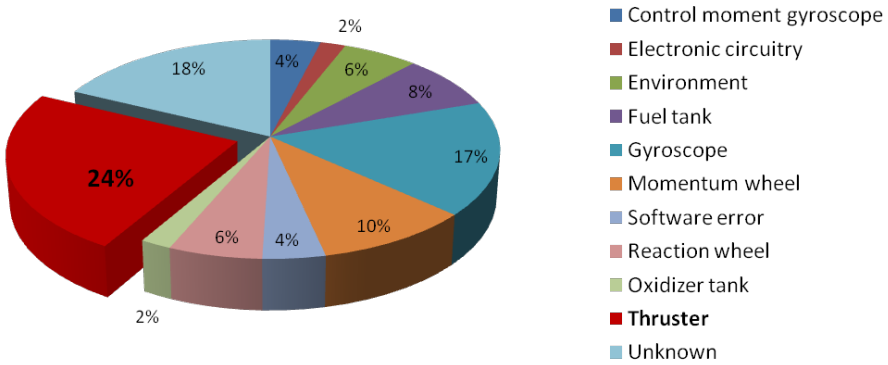


Figure 1 – Distribution of AOCS component faults

Table 1 lists some known on-orbit thruster failures occurred in a real spacecraft [109]. In most situations the occurrences of these faults could not be prevented, but subsequent analyses often

reveal that the consequences of faults could be avoided or, at least, that their severity could be significantly reduced.

Spacecraft	**Cause of the fault**	**Impact**
Galaxy 8i	During September 2000, three of four xenon ion thrusters failed [251]	Shortened mission life
Iridium 27	During September 1997, thruster anomaly depleted operational fuel [251]	Total mission loss
Nozomi	During December 1998, thruster valve was stuck partially open and the propulsion system consumed more fuel than expected during Earth swing-by [251]	Mission Interruption
JCSat-1B	During January 2005, the spacecraft experienced attitude loss during maneuver due to thruster anomaly [51]	Mission Interruption
EchoStar VI	During April 2001, the spacecraft was hit by one or more micrometeorites, in its attitude control system causing a propellant leak in one of the thrusters [272]	Mission Interruption

Table 1 – List of on-orbit thruster failures [109]

In general, there are many types of thruster failures that may occur in-flight. Since it is impractical and relatively hard to create a GNC system that is able autonomously to detect, isolate and accommodate any kind of thruster fault, it is important to prioritize those faults which most likely occur in-flight and have a large impact on the mission success and/or GNC performance. Fortunately, in many cases, possible faults can be known in advance from the Fault Mode and Effect Analysis (FMEA), but the number of FTC systems increases with the number of faults to be covered. A solution to this problem may consist in judiciously combining active FTC systems with passive fault tolerance principles (e.g., robust controller covering some marginal faults). As an example, the FMEA of the ATVs (Automated Transfer Vehicles) developed by EADS Space Transportation for the "Jules Verne" flight (docking the 3rd April 2003 and de-docking the 5th September 2008), revealed 32 000 cases of recovery to be analyzed. 20 000 were relevant cases according to the mission phase and 300 were recovery actions. This analysis took into account both the "function context" (breakdown in the functional units such as communication, data processing, power and propulsion systems) and the "vehicle context" (about 80 vehicle modes). As it is understood by the academic research community, only few of them were concerned by the FTC problem, since the majority dealt with FDIR problems.

The investigated faults in this thesis have been defined in accordance with ESA and TAS requirements and following their experiences. Four cases are particularly examined: *i*) thruster opening at 100% (in this case thruster provides maximum thrust regardless of the demand and is obviously very propellant consuming); *ii*) thruster stucks closed (in this case the faulty thruster does not generate any thrust regardless of the demanded command by the control authority); *iii*) small bi-propellant leakage and *iv*) loss of effectiveness of the specific thruster (i.e., the actual thrust is less than demanded).

It is obvious that, if for instance a fully open thruster fault occurs (thruster stucks fully open), it could lead to a drastic increase of the propellant consumption which is already very constrained by the travel to Mars. Furthermore, dramatic consequences can occur, e.g., the conventional GNC system may result in unsatisfactory performance and/or instability, possibly leading the chaser to lose the attitude and/or the position of the sample container. The problem becomes highly critical during the last 20 meters of the rendezvous phase when the chaser shall be cor-

rectly positioned in the rendezvous corridor in order to successfully capture the sample container, as well as, the chaser attitude needs to be maintained in the rendezvous sensor field of view. Such faulty situations obviously cannot be diagnosed by ground support using telemetry information, due to the potential lack of communication between the chaser and the ground stations and/or due to significant communication delay. Finally, to increase safety, reliability and mission success, the research topics should be motivated by applications and the results are for the applications. This motivates to conduct studies for the development of new on-board fully autonomous FTC solutions that shall cope with thruster faults which may occur and endanger the mission whilst maintaining the desirable degree of overall stability and performance.

Approach and Objectives

The ability to ensure the desired performance of a dynamic system both in the absence and presence of faults is an important task in many applications of control engineering. A cost-effective way to obtain increased reliability and safety in an autonomous spacecraft whilst keeping the desired performance level is to introduce active FTC approach. The basic implementation strategy of an active FTC system involves the design of a model-based Fault Detection and Isolation (FDI) unit that monitors the behavior of the components such that local incipient faults are prevented from developing into severe failures that can lead to a total mission loss. A quick detection and isolation of these faults is the first step towards an efficient fault accommodation action. The algorithmic simplicity in detecting and isolating faults is also a very important aspect when considering the need for validation and on-board implementation of a demonstrable scheme. Only very few FTC algorithms that meet the above requirements have been developed in practice and applied to a real spacecraft.

One possibility of detecting a thruster fault is through the use of specialized pressure and temperature sensors in the nozzle of a thruster. This, however, comes at the price of extra mass, cost and complexity. This thesis instead focuses on solutions of performing thruster FDI using only additional software and hardware already on board. Thus, the aim of this thesis is to propose a complete model-based FDI/FTC system able to quickly detect, isolate and accommodate a single thruster fault and therefore significantly increase the operational autonomy and safety of the chaser during the rendezvous and more generally, of any spacecraft involved in a deep space mission. Since redundancy exists in the sensors and since the reaction wheels are not used during the terminal rendezvous sequence, the work presented in this thesis deals only on the thruster-based propulsion system.

Thruster fault accommodation (recovery) is traditionally achieved through a fully redundant thruster set or through an overactuation (functional redundancy). After a thruster fault has been successfully detected or eventually isolated, the system can attempt to recover from faults. In general, four tolerance principles against thruster faults can be distinguished:

1. Thruster fault compensation;
2. Completely switching to a redundant thrusters set (requires only fault detection);
3. Switching to a thruster in the redundant thruster set;
4. Control using the remaining N-1 thrusters;

It is obvious, that the first principle would possibly lead to a drastic increase of the propellant consumption, which is already very constrained by the travel to Mars, and thus greatly reducing the spacecraft lifetime and mission success. The second principle does not require any isolation function, but on the other hand significantly decrease the fault coverage capabilities since only one single fault can be recovered at all. Moreover, it requires a fully redundant thruster set which obviously add extra mass, volume and complexity to the spacecraft, and therefore reducing payload and increasing the cost. Without a dedicated valve to shut off the faulty thruster, the only way to control the spacecraft is through the first two principles, however, if each thruster is equipped with a dedicated thruster valve that can disconnect the propellant supply into it, it is possible to consider the third and fourth principle. The third principle still requires a full thruster redundancy, but in this approach more than one thruster can be considered faulty. The last principle requires a functional redundancy thruster set. Here, the fault tolerance relies on a control redistribution approach, which aims at reallocating the desired control effort among the remaining N-1 healthy actuators. The advantage of this approach is the reduced number of thrusters (no redundant set) and therefore mass, volume and complexity savings. Due to the above mentioned and also other obvious reasons explained later, the focus of this thesis will only be on methodologies which involves the third and fourth principles only.

Overview of the Chapter Contents

This thesis is comprised of four chapters and is organized as follows:

The first chapter provides a literature review of the main approaches in the field of model-based fault diagnosis and active fault-tolerant control. It also comes with a decent list of bibliographical references for the main contributions. Application examples from the space community, that have been successfully demonstrated in flight or in high-fidelity industrial simulators, are presented where applicable. The chapter is concluded by a summary-like table introduced in order to compare the presented approaches according to some pre-selected criteria.

The second chapter briefly describes the Mars Sample Return mission, its rendezvous phase and the vehicles involved in the mission. It describes the GNC unit, that is in charge of controlling the chaser during the rendezvous phase and the failure management unit, that is in charge of detecting failures and of engaging corrective maneuvers. It is shown how the FDIR and FTC solutions investigated in the next chapters can be integrated in the failure management unit. This chapter also addresses the models of the chaser spacecraft dynamics (relative position between the chaser and the target and chaser's attitude), that will be further used in the following chapters to design model-based FDIR/FTC solutions. Modelling of the chaser spacecraft thruster-based propulsion is also addressed to outline the effect of the faults. Necessities on modeling the spacecraft dynamics during the rendezvous phase as well as the rendezvous requirements in terms of GNC performance and successful capture are introduced.

The third chapter is dedicated to the development of a FDIR solution for thruster fault recovery. It introduces the baseline thruster configuration of the chaser consisting of a nominal and a fully redundant thruster set. The design of two distinct model-based FDIR techniques able to detect, isolate and accommodate (recover) a single thruster fault is addressed. The first approach is based on the position model whereas the second approach is based on the attitude model. Both techniques focus on the robustness issue against the unknown time-varying delays induced by the propulsion drive electronics and uncertainties on thruster rise times. A complete

description of a robust residual generation design approach based on Eigenstructure Assignment (EA) technique is discussed in details. Computational procedure and implementation issues of the FDI schemes design are carefully discussed. A fault accommodation strategy, achieved by employing the additional hardware redundancy in the thruster-based propulsion system, is proposed. Finally, Monte Carlo (MC) results demonstrate the feasibility and efficiency of the proposed schemes. Carefully selected performance and reliability indices allow to compare the effectiveness of both approaches. Recovery aspects are also studied.

The fourth chapter addresses a different thruster configuration with functional redundancy. For this configuration, an innovative active FTC strategy is proposed to unambiguously detect, isolate and accommodate any kind of the considered thruster faults. Key features of the given method are the use of a fault detector based on EA technique for robust and quick fault detection, a bank of Nonlinear Unknown Input Observers (NUIO) with dynamics assignment together with an Extended Kalman Filter-based torque bias estimator for fault isolation. An online Control Allocation (CA) algorithm scheduled by the fault isolation scheme is proposed for fault tolerance. A MC campaign is conducted in the context of the terminal rendezvous phase. Mission oriented criteria demonstrate that the proposed FTC strategy is able to cope with a large class of thruster faults despite the presence of various types of uncertainties.

This PhD was performed in the frame of ESA Networking/Partnering Initiative (NPI) sponsored project for "Model-based Fault Diagnosis and Fault Accommodation for Space Missions", contract number 149-2010, supported during three years by ESA and Thales Alenia Space.

Chapter 1

State of the Art in Model-based Fault Diagnosis and Active Fault-tolerant Control

"It takes a wise man to learn from his mistakes, but an even wiser man to learn from others."
— Zen proverb

The aim of this chapter is to provide the reader with an overview of the main techniques in the fields of model-based fault diagnosis and active fault-tolerant control. A decent list of bibliographical references for the main contributions is provided too. Application examples of the methods, that have been successfully demonstrated in flight or in high-fidelity simulators, are presented from the space community where applicable. A summary-like table is presented as a conclusion in order to compare the presented techniques according to some pre-selected criteria.

1.1 Introduction

Fault-tolerance in dynamic systems is traditionally achieved through the use of hardware redundancy. Repeated hardware units (actuators, sensors, process components, etc.) are usually distributed spatially around the system to provide protection against localized damage. Such schemes operate typically in a duplex, triplex or quadruplex redundancy configuration and redundant outputs (or measurements) are compared for consistency. For example, three (or more) sensors measuring the same variable are installed where one would be sufficient if it was entirely reliable. The signals from these sensors are monitored by a logical system which neglects small differences in the signals due to noise, manufacturing tolerances of the measurement instruments, but which declares that a sensor is faulty if its signal deviates too far from the average value of the others (assuming that the others remain within a small differences from one another). This approach to fault-tolerance is simple and widely used. In some cases, it can be reasonably straightforward to apply. It is essential in the control of aircraft, space vehicles and in certain

process plants. The major problems related to the hardware redundancy are the extra cost and the additional space required to accommodate the equipment. In spacecraft, for example, the additional space could be used for more mission-oriented equipment (scientific devices, reserve propellant, etc.).

Safety-critical applications (such as space vehicles, aircrafts, power plants, cars, rapid transit trains, etc.) of which reliability, availability and operating safety are primary design requirements, application of ultra-high dependable control systems is needed. For such systems, an important means of increase in dependability is to detect and identify the different types of faults, and then to accommodate or minimize the impact of them. A control system with this kind of fault-tolerance capability is defined as a Fault-Tolerant Control System (FTCS).

The FTCS tasks are typically three or four. The first task is the *fault detection*. Fault detection indicates the occurrence of a certain fault in a monitored system. The second task is called *fault isolation* which determines the type and/or location of the fault. This two tasks are in literature referred with the common term Fault Detection and Isolation (FDI). Once the fault is isolated, then the task of *fault identification* might be considered, too. Fault identification aims at determining the magnitude and shape of a fault. The term Fault Detection and Diagnosis (FDD) is an extension of the term FDI in the sense that the procedures of FDD provide an additional "diagnosis" to the faults in terms of fault identification and sometimes an assessment of the degree of severity of the fault. In other words, FDD is mainly used to underline the need for fault estimation. After the fault is detected and diagnosed, in some applications fault is accommodated (i.e., a self-correcting of the fault) is required, usually through controller redesign.

Over the last decades, the growing demand for safety, reliability, and maintainability in technical systems has drawn significant research interest in FDI and FDD. Such efforts have led to the development of many essential techniques, see for example the survey works [19, 60, 93, 96, 135, 168, 210, 223, 224, 284]. Research on reconfigurable Fault-tolerant Control (FTC) has increased progressively since the initial research on restructurable control and self-repairing flight control systems of the early 1980s appeared [36, 84]. More recently, FTC has attracted more and more attention, in both industry and academic communities [319], due to increased demands for safety, high system performance, productivity and operating efficiency in a wider engineering applications. Several survey literature on FTCS have been published [16, 17, 19, 78, 143, 148, 268, 285, 312].

1.2 General Procedure of Fault-tolerant Control Systems

Generally speaking, fault-tolerant control systems can be classified into two main types based on different methodologies [312]:

- **Passive Fault-tolerant Control Systems (PFTCS)**
  In PFTCS, controllers are fixed and designed to be robust against a class of presumed faults [84]. This approach needs neither FDD schemes nor controller reconfiguration, but it has limited fault-tolerant capabilities [312]. Fault-tolerance is obtained without changing the default controller parameters, therefore it is called *passive fault tolerance*. From a classical control theory perspective, passive FTC is close to robust control. Furthermore, a robust controller works suboptimal for the nominal plant because its parameters are fixed so as to

get a trade-off between performance and robustness [19]. Further discussions on PFTCS are beyond the scope of this work and interested readers are referred to [176, 207, 283, 312] and the references therein.

- **Active Fault-Tolerant Control Systems (AFTCS)**
  In contrary to PFTCS, AFTCS acts to the system component failures actively by controller re-design so that the stability and acceptable performance of the entire system can be verified. Indeed, most of the earlier works on AFTCS design deal with the problem of recovering the pre-fault (before the fault occurs) system performances as much as possible [2, 209, 224]. The great benefit of the AFTCS approaches is that the fault-tolerance does not degrade the performance level in normal (fault-free) operating mode. From a classical control theory point of view, AFTCS can be seen as an adaptive control scheme that reacts to the fault event. This is the type of FTCS which we will present in Chapter 4 of this thesis.

The architecture of a general AFTCS is depicted in Fig. 1.1. The two blocks "diagnostic module" and "controller re-design" carry out the two steps of the fault tolerance. These two blocks operate in a supervision level. In AFTCS, the information obtained from the diagnostic module is used in the controller re-design [210]. Hence, system diagnostic module with its diagnostic algorithms should not only indicate that some faults have occurred but it has to identify the fault locations (i.e., to do FDI) and in some cases the fault magnitude and the shape (i.e., to do FDD) of the fault signal with sufficient precision [276]. The re-design block uses the fault information and make it possible to set up a model of the faulty system, which can be used to determine the appropriate control law. "Appropriate" is meant with respect to given objectives which depend on the application, but which in all cases must preserve stability [151].

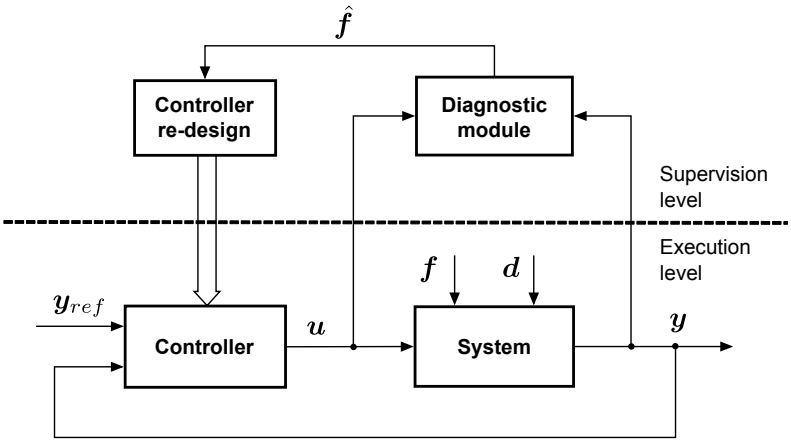


Figure 1.1 – General architecture of an active fault-tolerant control system [19]

The figure above shows also that the AFTCS extends the regular feedback controller by a supervision level, which includes the diagnostic module (FDI and/or FDD) and the controller re-design blocks. In the fault-free case, the nominal controller attenuates the disturbances d and ensures following the reference signal y_{ref} and other performance requirements on the closed-loop system. In fault-free case, the diagnostic module simply recognizes that the system is not suffering from any faults and no change in the control law is required. If a fault f occurs, the supervision level makes the control loop fault-tolerant, i.e., the diagnostic module identifies the fault and the controller re-design block will try to change the control law in order to cope with the faulty situation. Afterwards, the execution level alone continues to satisfy the control

objectives [19].

Controller re-design considers the problem of changing the controller parameters and/or the control structure after a fault has been diagnosed in the system. The goal is to satisfy the requirements on the closed-loop system despite the presence of faults. In principal, two ways of controller re-design have to be distinguished [17, 19, 151, 224].

Fault Accommodation

Fault accommodation means to adapt the controller parameters to the dynamical properties of the faulty system. The input and output of the system used in the control loop remain the same as for the fault-free case. The response to the diagnosed faults should be an adequate change of the controller parameters. The main problem addressed in this approach is to calculate these new parameters. This step is usually performed on-line, therefore fault accommodation is usually autonomous [267]. A formal definition of the fault accommodation can be found in Blanke et al. [17, 19].

A simple, but well established way of fault accommodation is based on pre-designed controllers, each of which has been calculated off-line for a specific fault. The re-design step then simply sets the switch among the different control laws. However, the activation/repair mechanism may happen too quickly and during the whole operation interval which may cause instability of the control law [80] and might lead to strong real-time constraints [19].

Moreover, the controller re-design has to be made for all possible faults before the system is put into operation and all resulting controllers have to be stored in the control software. Fortunately, in many systems, possible faults are known in advance from the Fault Mode and Effect Analysis (FMEA), but the number of FTC systems increases with the number of faults to cover. A solution to this problem may consist in judiciously combining PFTCS and AFTCS as it is proposed by Staroswiecki and Berdjag [266]. In case of severe faults that change the structure of the system, this approach is no more sufficient because the structure of the controller is not changed.

Control Reconfiguration

Control reconfiguration is usually necessary in the event of severe faults, such as total failures in actuators/sensors. If these components fail completely, the fault leads to a break-down of the control loop. There is no possibility to adapt the controller by simply changing its parameters to the faulty situation, i.e., a complete control loop has to be reconfigured. A new control law has to be selected and the controller structure has to be changed where alternative actuators and sensors have to be found, which are not affected by the fault, and which are able to satisfy the stability and the performance specifications on the closed-loop system. Note that the pre-computed FTC solutions mentioned previously can be a viable approach in this case.

Remark 1.1. *An important question in the controller re-design step is the analysis of* reconfigurability *as a system property. Reconfigurability is a property of faulty systems meaning that the original control goals specified for the fault-free system can be reached after suitable control re-design. A structural analysis of the reconfigurability can be found in [104]. The work of Staroswiecki [263] deals with the reconfigurability on a linear level, based on the solvability of an optimal control problem with minimal control energy.*

Remark 1.2. *The term Fault/Failure Detection, Isolation and Recovery (FDIR) is widely used in the industrial community when referring to FTC approaches.*

System and Fault Modeling

Faults occurring in a system can be generally classified into three types [19, 97, 145, 284]:

- actuator faults;
- sensor faults; and
- component faults.

Actuator and sensor faults are typically referring to faults/failures occurring in the system actuation and measurement system/subsystems. Component faults usually lead to changes in the parameters of the system dynamics. Figure 1.2 illustrates a general fault model in the open-loop system with actuator, system component and sensor faults, respectively.

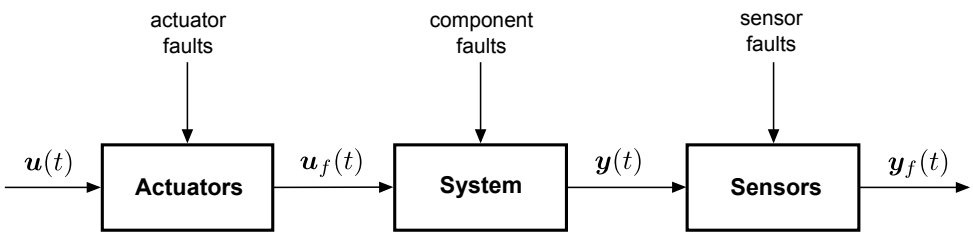


Figure 1.2 – Open-loop system with different types of faults

Faults can be categorized into *additive faults* and *multiplicative faults*, where the additive faults are described as additional functions, which are added in the system dynamical equations (see (1.1) and (1.4)), while the multiplicative faults are represented by the product of a variable with the faults [10, 145] (see (1.6), (1.5) and (1.2)).

Ignoring the actuator dynamics, vector $\boldsymbol{u}_f \in \mathbb{R}^{n_u}$ of the faulty controlled system input can be described in terms of an additive fault type, i.e.,

$$\boldsymbol{u}_f(t) = \boldsymbol{u}(t) + \boldsymbol{f}_a(t) \tag{1.1}$$

where $\boldsymbol{u} \in \mathbb{R}^{n_u}$ is the actuator control input and $\boldsymbol{f}_a \in \mathbb{R}^{n_u}$ represents the additive actuator fault vector. With regards to modelling multiplicative actuator faults, the following model can be used [128]

$$\boldsymbol{u}_f(t) = \big(\boldsymbol{I} - \boldsymbol{\Psi}(t)\big)\boldsymbol{u}(t) \tag{1.2}$$

where $\boldsymbol{\Psi} = \mathrm{diag}(\psi_1, \ldots, \psi_{n_u})$ is an unknown matrix and ψ_i models to the ith actuator fault. For instance, $\psi_i = 1$ means that the ith actuator is out of order and $\psi_i = x\%$ means a loss of efficiency of $x\%$ of the ith actuator. Note that if the controlled system keeps stability, then the multiplicative-based model can be approximated in terms of an additive fault model according to [97]

$$\boldsymbol{u}_f(t) = \boldsymbol{u}(t) - \boldsymbol{\Psi}(t)\boldsymbol{u}(t) = \boldsymbol{u}(t) + \boldsymbol{f}_a(t) \tag{1.3}$$

Without taking into account sensor dynamics, the faulty measured output vector $\boldsymbol{y}_f \in \mathbb{R}^{n_y}$ can be described as

$$\boldsymbol{y}_f(t) = \boldsymbol{y}(t) + \boldsymbol{f}_s(t) \tag{1.4}$$

where $\boldsymbol{y} \in \mathbb{R}^{n_y}$ is the true output vector of the system and $\boldsymbol{f}_s \in \mathbb{R}^{n_y}$ represents a vector of additive sensor faults. Similarly to the actuator case, the multiplicative faults model admits the following representation

$$\boldsymbol{y}_f(t) = (\boldsymbol{I} - \boldsymbol{\Psi}(t))\boldsymbol{y}(t) \tag{1.5}$$

that can be approximated according to (1.4).

The component faults are commonly modelled as multiplicative faults, i.e., they are modelled as changes in the parameters of the system matrices. In the linear case and under the assumption that the (controlled) system keeps stability, the ith row and j^{th} column element a_{ij} of the system matrix $\boldsymbol{A}$ represents a system parameter change, then the component fault can be described as follows

$$\boldsymbol{f}_c(t) = \boldsymbol{I}_i \Delta a_{ij} x_j(t) \tag{1.6}$$

where x_j is the jth element of the state vector $\boldsymbol{x} \in \mathbb{R}^{n_x}$, $\boldsymbol{I}_i$ is vector with all zero elements except '1' in the ith element and Δa_{ij} represents the parameter change around the nominal value a_{ij}.

1.3 Methods for Fault Detection and Isolation

There is a great variety of fault detection and isolation methods, e.g., the parity space approach [106], methods based on unknown input observer concepts [39], the multiple model method [28], the geometric approach for detection filter design [190], or methods based on frequency domain concepts [95]. According to Frank [93], a great variety of methods exists in the literature and they can be brought down to a four basic classes as follows:

- parity space approach [47, 64, 93, 105, 193, 227].
- observer-based approach and innovation-based approach [19, 60, 93, 96, 103, 210, 228],
- parameter identification approach [144, 260, 305], and
- fault detection filter approach [10, 19, 128, 132, 270].

All these four methods are discussed in more detail in the following sections. Since linear approaches are special cases of nonlinear methods, nonlinear approaches are preferred. Examples from space systems are given where available.

1.3.1 Parity Space Approach

The concept of the parity relation-based fault detection approach is to check the parity, i.e., consistency of the mathematical equations (analytical redundancy) of the system by using the actual measurements. A fault is declared to have occurred once given error bounds are exceeded. Some parity space approaches are able to achieve fault isolation properties [193]. Several survey papers have been written on parity relation based fault detection methods [47, 93, 105, 227].

The following developments give an overview of the general method. Using physical laws, a large class of engineering systems can be modelled by differential equations of the form

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{h}(\boldsymbol{x}(t), \boldsymbol{u}(t), \boldsymbol{f}(t), \boldsymbol{d}(t)) \\ \boldsymbol{y}(t) = \boldsymbol{g}(\boldsymbol{x}(t), \boldsymbol{u}(t), \boldsymbol{f}(t), \boldsymbol{d}(t)) \end{cases} \tag{1.7}$$

where $\boldsymbol{h} \in \mathbb{R}^{n_x}$ and $\boldsymbol{g} \in \mathbb{R}^{n_y}$ are smooth[1] nonlinear vector functions of their arguments, $\boldsymbol{x} \in \mathbb{R}^{n_x}$ is the state vector, $\boldsymbol{u} \in \mathbb{R}^{n_u}$ the input vector, $\boldsymbol{y} \in \mathbb{R}^{n_y}$ the vector of measured outputs, $\boldsymbol{d} \in \mathbb{R}^{n_d}$ the vector of unknown inputs and $\boldsymbol{f} \in \mathbb{R}^{n_f}$ the vector of faults.

Assuming that the functions $\boldsymbol{h}$ and $\boldsymbol{g}$ are differentiable up to order s_h, the following yields

$$\bar{\boldsymbol{y}}^{(s_h)}(t) = \boldsymbol{G}^{s_h}(\boldsymbol{x}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) \tag{1.8}$$

where

$$\boldsymbol{G}^{s_h}(\boldsymbol{x}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) = \begin{pmatrix} \boldsymbol{g}(\boldsymbol{x}(t), \boldsymbol{u}(t), \boldsymbol{f}(t), \boldsymbol{d}(t)) \\ \boldsymbol{g}_1(\boldsymbol{x}(t), \bar{\boldsymbol{u}}^{(1)}(t), \bar{\boldsymbol{f}}^{(1)}(t), \bar{\boldsymbol{d}}^{(1)}(t)) \\ \vdots \\ \boldsymbol{g}_{s_h}(\boldsymbol{x}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) \end{pmatrix}$$

If the system (1.8) is solvable with respect to $\boldsymbol{x}$, then it can be written in the equivalent form

$$\boldsymbol{x}(t) = \boldsymbol{G}_x(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) \tag{1.9}$$

$$\boldsymbol{G}_y(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) = \boldsymbol{0} \tag{1.10}$$

It can be seen, that (1.10) is an analytical redundancy relation, independent of the state vector $\boldsymbol{x}$. In fault-free operation, it yields the necessary condition

$$\boldsymbol{G}_y(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \boldsymbol{0}, \bar{\boldsymbol{d}}^{(s_h)}(t)) = \boldsymbol{0} \tag{1.11}$$

If the function $\boldsymbol{G}_y(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t))$ can be written as the difference of two functions $\boldsymbol{G}_y^c$ and $\boldsymbol{G}_y^e$, such as

$$\begin{aligned} &\boldsymbol{G}_y(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) = \\ &= \boldsymbol{G}_y^c(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t)) - \boldsymbol{G}_y^e(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) \end{aligned} \tag{1.12}$$

Then, it is possible to construct the residual $\boldsymbol{r}$ as follows

$$\boldsymbol{r}(t) = \boldsymbol{G}_y^c(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t)) = \boldsymbol{G}_y^e(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) \tag{1.13}$$

where $\boldsymbol{G}_y^c$ is the computation form and $\boldsymbol{G}_y^e$ is the evaluation form of the residual, respectively. The necessary condition for proper operation becomes

$$\boldsymbol{r}(t) = \boldsymbol{G}_y^c(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t)) = \boldsymbol{G}_y^e(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \boldsymbol{0}, \bar{\boldsymbol{d}}^{(s_h)}(t)) = \boldsymbol{0} \tag{1.14}$$

Remark 1.3. *If the disturbances are governed by a stochastic model with zero mean, the residual*

[1] A smooth function has continuous partial derivatives of any order with respect to its arguments

(1.14) *will be, generally, non-zero mean in the absence of faults, since it is linked to disturbances in a nonlinear manner.*

Finally, by decomposing the fault vector $\boldsymbol{f}$ and the disturbance vector $\boldsymbol{d}$

$$\boldsymbol{f}(t) = \begin{pmatrix} \boldsymbol{f}_1(t) \\ \boldsymbol{f}_2(t) \end{pmatrix}, \qquad \boldsymbol{d}(t) = \begin{pmatrix} \boldsymbol{d}_1(t) \\ \boldsymbol{d}_2(t) \end{pmatrix} \tag{1.15}$$

then the fundamental problem of designing robust and structured residuals boils down to the solvability of the problem

$$\boldsymbol{G}_y(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) = \boldsymbol{0} \tag{1.16}$$

with respect to $\bar{\boldsymbol{f}}(t)^{(s_h)}$ and $\bar{\boldsymbol{d}}(t)^{(s_h)}$, the following equivalence yields

$$\boldsymbol{G}_y^1(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}_1^{(s_h)}(t), \bar{\boldsymbol{d}}_1^{(s_h)}(t), \bar{\boldsymbol{f}}_2^{(s_h)}(t), \bar{\boldsymbol{d}}_2^{(s_h)}(t)) = \boldsymbol{0} \tag{1.17}$$

$$\boldsymbol{G}_y^2(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}_2^{(s_h)}(t), \bar{\boldsymbol{d}}_2^{(s_h)}(t)) = \boldsymbol{0} \tag{1.18}$$

If the second relation (1.18) can be written as a difference

$$\begin{aligned} &\boldsymbol{G}_y^2(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}_2^{(s_h)}(t), \bar{\boldsymbol{d}}_2^{(s_h)}(t)) = \\ &= \boldsymbol{G}_y^{2c}(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t)) - \boldsymbol{G}_y^{2e}(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}_2^{(s_h)}(t), \bar{\boldsymbol{d}}_2^{(s_h)}(t)) \end{aligned} \tag{1.19}$$

then, as in (1.12), the residual (structured and robust) verify that

$$\boldsymbol{r}(t) = \boldsymbol{G}_y^{2c}(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t)) = \boldsymbol{G}_y^{2e}(\bar{\boldsymbol{y}}^{(s_h)}(t), \bar{\boldsymbol{u}}^{(s_h)}(t), \bar{\boldsymbol{f}}^{(s_h)}(t), \bar{\boldsymbol{d}}^{(s_h)}(t)) \tag{1.20}$$

where again $\boldsymbol{G}_y^{2c}$ is the computation form and $\boldsymbol{G}_y^{2e}$ is the evaluation form.

Remark 1.4. *From a practical point of view, it should be noted that it is not necessary to derive all outputs to the same order. A set of equations can be obtained by comparing the derivatives y_1 up to the order s_1, y_2 up to the order s_2, etc.. The only constraint is that the set of obtained equations $(s_1 + s_2 + \ldots)$ meets the solvability conditions necessary and sufficient for the existence of an analytical redundancy relations for the desired decoupling.*

- **Application to Space Missions**

The most common application of parity space methods in the aerospace field is based on the redundancy available in Inertial Measurement Units (IMUs). The redundant measurements acquired from the IMUs are used for deriving the so-called parity-space relations. In particular, three configurations are used, i.e., the octahedron, dodecahedron and dedicated pyramidal configurations, see Fig. 1.3 for an illustration [135].

In the octahedron configuration, each axis (labelled numerically 1 through 6) contains a gyro and an accelerometer. Complementary axes (i.e., 1 and 2; 3 and 4; and 5 and 6) make angles of 90 deg with each other and are symmetrically placed with respect to the body frame. Consequently instruments 1 and 2 are both inclined 45 deg with respect to the z body axis. Instruments 3 and 4 are inclined 45 deg with respect to the x body axis and 5 and 6, 45 deg with respect to the y body axis. This configuration facilitates the determination of 7 (static) parity relations

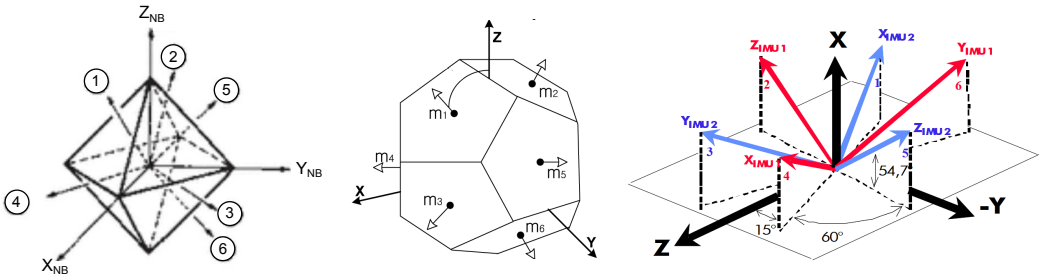


Figure 1.3 – The octahedron (left), the dodecahedron (centre) and the dedicated pyramid (right) configurations [135]

defined as functions of the measurements $m_1, \ldots, m_6$ according to

$$
\begin{aligned}
r_1 &= m_1 - m_2 - m_3 - m_4 \\
r_2 &= m_2 + m_3 - m_5 \\
r_3 &= m_6 + m_1 - m_3 \\
r_4 &= m_4 + m_5 - m_1 \\
r_5 &= m_4 + m_6 + m_2 \\
r_6 &= m_1 + m_2 + m_6 - m_5 \\
r_7 &= m_4 + m_5 + m_6 - m_3
\end{aligned}
$$

These equations are used to detect and isolate a single axis fault in either gyros or accelerometers or a simultaneous correlated double axis fault.

The dedicated pyramidal configuration is based on two IMUs arranged in a geometric configuration, so that any single failure (1-axis gyro or 1-axis accelerometer) can be detected and isolated, through the 7 following (static) parity relations

$$
\begin{aligned}
r_1 &= (m_1 + m_4) - (m_2 + m_5) \\
r_2 &= (m_2 + m_5) - (m_3 + m_6) \\
r_3 &= (m_3 + m_6) - (m_1 + m_4) \\
r_4 &= 2(m_1 + m_3 + m_5) - 3(m_1 + m_4) \\
r_5 &= 2(m_2 + m_4 + m_6) - 3(m_1 + m_4) \\
r_6 &= 2(m_1 + m_3 + m_5) - 3(m_2 + m_5) \\
r_7 &= 2(m_2 + m_4 + m_6) - 3(m_2 + m_5)
\end{aligned}
$$

where measurements m_1, m_3, m_5 are for IMU1 and m_2, m_4, m_6 are for IMU2. For the fault detection purpose, only $r_i, i = 1, 2, 3$ are used whereas the four last signals $r_i, i = 4, \ldots, 7$ are used for fault isolation in gyros and accelerometers. The dedicated pyramidal configuration FDI technique is used in the Mars Sample Return mission, see discussion in Chapter 2.

1.3.2 Observer-based Approaches

Observer-based methods are the most popular form of model-based residual generator approaches. The basic idea is to estimate the output vector of the system (the state vector is usually unnecessary) from the measurements or from a subsets of the measurements. Then the estimation error or innovation is used to form a residual signal for fault detection and/or

isolation. It is well known from observer theory that for state estimation one can use linear or nonlinear, full or reduced-order state observers in the deterministic case or Kalman filters in the stochastic case when noise has to be considered. Many different design approaches have been employed [60, 93, 96, 103, 228, 308]. In the following developments, focus is on robust methods.

1.3.2.1 Iterative Learning Observer

This kind of observer is different from conventional Luenberger observer where the observer state is only a function of the actual input, output and the estimation error. Iterative Learning Observer (ILO) performs state estimation updated online by past system output errors as well. For the purposes of FDD, an ILO is used for jointly estimate the system state and the fault.

To proceed, let the system be modelled by the following class of nonlinear state space model

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{g}(\boldsymbol{x}(t)) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{E}_f\boldsymbol{f}(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{1.21}$$

where the vector function $\boldsymbol{f}$ denotes an additive time varying signal that models the faults to be estimated. It is assumed that $\boldsymbol{f}$ is bounded and that $\|\boldsymbol{f}(t) - \boldsymbol{K}_1\boldsymbol{f}(t-\tau)\|_\infty$ is finite. The structure of the ILO is then defined according to

$$\begin{cases} \dot{\hat{\boldsymbol{x}}}(t) = \boldsymbol{g}(\hat{\boldsymbol{x}}(t)) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{L}(\boldsymbol{y}(t) - \boldsymbol{C}\hat{\boldsymbol{x}}(t)) + \boldsymbol{E}_f\boldsymbol{v}(t) \\ \boldsymbol{v}(t) = \boldsymbol{K}_1\boldsymbol{v}(t-\tau) + \boldsymbol{K}_2(\boldsymbol{y}(t) - \boldsymbol{C}\hat{\boldsymbol{x}}(t)) \end{cases} \tag{1.22}$$

where $\boldsymbol{L}$, $\boldsymbol{K}_1$, $\boldsymbol{K}_2$ are gain matrices to be designed. The parameter τ is the sampling time interval (updating interval). The signal $\boldsymbol{v}$ is the ILO input that is used to estimate the time-varying fault. It can be seen that $\boldsymbol{v}$ is updated by both its past information and the output estimation error.

Several papers are devoted to the problematic of designing an ILO. For example, the work of Chen and Saif [41] deals with the design of an ILO-based approach to fault detection and fault accommodation in nonlinear systems. An ILO approach for robust fault detection is proposed in [42]. Industrial application of fault diagnosis in satellite systems for estimation of time-varying thruster faults can be found in [44].

1.3.2.2 Unknown Input Observer

The basic idea behind the Unknown Input Observer (UIO) approach is the construction of a vector $\boldsymbol{z}$ decoupled from disturbances as well as uncertainties which are expressed in terms of unknown input signals.

One of the most general theory was initially proposed by [257, 258]. In that approach, faults to be detected are represented by exogenous input signals (additive fault types). The model is considered to be nonlinear with respect to the state $\boldsymbol{x}$ and control signal $\boldsymbol{u}$, but linear with respect to faults and to all unknown inputs as follows

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{h}(\boldsymbol{x},\boldsymbol{u}) + \boldsymbol{K}(\boldsymbol{x},\boldsymbol{u})\boldsymbol{f}(t) + \boldsymbol{E}(\boldsymbol{x})\boldsymbol{d}(t) \\ \boldsymbol{y}(t) = \boldsymbol{g}(\boldsymbol{x}) \end{cases} \tag{1.23}$$

$\boldsymbol{h}$ and $\boldsymbol{g}$ are nonlinear vector functions of their arguments, $\boldsymbol{x} \in \mathbb{R}^{n_x}$ is the state vector, $\boldsymbol{u} \in \mathbb{R}^{n_u}$ the input vector, $\boldsymbol{y} \in \mathbb{R}^{n_y}$ the vector of measured outputs, $\boldsymbol{d} \in \mathbb{R}^{n_d}$ the vector of unknown inputs to be decoupled and $\boldsymbol{f} \in \mathbb{R}^{n_f}$ the vector of faults. $\boldsymbol{E}(\boldsymbol{x})$ and $\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{u})$ are respectively the unknown inputs and faults distribution vector functions of appropriate dimensions. It is assumed that $\boldsymbol{x}(t) \in \mathcal{C}$, $\forall t \geq 0$, where $\mathcal{C} \subseteq \mathbb{R}^{n_x}$ is compact, connected, has a nonempty interior and contains $\mathbf{0}$.

The approach proposed by [257, 258] consists in finding a nonlinear state transformation $\boldsymbol{z} = \boldsymbol{T}(\boldsymbol{x})$ in order to separate the disturbed from the undisturbed portion of the model. This can be met if the following condition holds

$$\frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}} \boldsymbol{E}(\boldsymbol{x}) = \mathbf{0} \tag{1.24}$$

This relation constitutes a system of first order linear partial differential equations which are to be solved simultaneously by $\boldsymbol{z} = \boldsymbol{T}(\boldsymbol{x})$. The theorem of Frobenius [149] can be applied to derive necessary and sufficient existence conditions for the solution of (1.24):

Theorem 1.1. *Assume that the rank of $\boldsymbol{E}(\boldsymbol{x})$ is equal to n_q for all $\boldsymbol{x}$. Then the searched transformation $\boldsymbol{T}(\boldsymbol{x})$ is a $(n_x - n_q)$ vector, solution of the following system*

$$\frac{\partial \boldsymbol{T}_i(\boldsymbol{x})}{\partial \boldsymbol{x}} \boldsymbol{E}(\boldsymbol{x}) = \mathbf{0}, \quad i = 1, ..., n_x - n_q \tag{1.25}$$

where $\boldsymbol{T}_i(\boldsymbol{x})$ denote the ith row of $\boldsymbol{T}(\boldsymbol{x})$. Furthermore, there exists $n_x - n_q$ independent $\boldsymbol{z}_i = \boldsymbol{T}_i(\boldsymbol{x}), \quad i = 1 \ldots n_x - n_q$ if and only if

$$\operatorname{rank}\Big(\boldsymbol{E}(\boldsymbol{x}) \quad [\boldsymbol{e}_i(\boldsymbol{x}), \boldsymbol{e}_j(\boldsymbol{x})]\Big) = n_q, \quad \forall i, j = 1 ... n_q \tag{1.26}$$

where $\boldsymbol{e}_i(\boldsymbol{x})$ denotes the ith column of $\boldsymbol{E}(\boldsymbol{x})$ and $[\boldsymbol{e}_i(\boldsymbol{x}), \boldsymbol{e}_j(\boldsymbol{x})]$ refers to the Lie bracket of two elements, i.e.,

$$[\boldsymbol{e}_i(\boldsymbol{x}), \boldsymbol{e}_j(\boldsymbol{x})] = \frac{\partial \boldsymbol{e}_j(\boldsymbol{x})}{\partial \boldsymbol{x}} \boldsymbol{e}_i(\boldsymbol{x}) - \frac{\partial \boldsymbol{e}_i(\boldsymbol{x})}{\partial \boldsymbol{x}} \boldsymbol{e}_j(\boldsymbol{x}), \quad i, j = 1 \ldots n_q \tag{1.27}$$

In order to obtain the transformed (decoupled) model, the decoupled state $\boldsymbol{z}$ must be augmented by a subset of measurements $\bar{\boldsymbol{y}} = \boldsymbol{\phi}(\boldsymbol{y})$ such that a relation $\boldsymbol{x} = \boldsymbol{\psi}_0(\boldsymbol{z}, \bar{\boldsymbol{y}})$ exists, where $\dim(\bar{\boldsymbol{y}}) < \dim(\boldsymbol{y})$. The conditions of the existence of $\boldsymbol{\psi}_0(\boldsymbol{z}, \bar{\boldsymbol{y}})$ are

$$\operatorname{rank}\begin{pmatrix} \frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}} \\ \frac{\partial \boldsymbol{\phi}(\boldsymbol{y})|_{\boldsymbol{y}=\boldsymbol{g}(\boldsymbol{x})}}{\partial \boldsymbol{x}} \end{pmatrix} = n_x \tag{1.28}$$

$$\lim_{\|\boldsymbol{x}\| \to \infty} \| \Big(\boldsymbol{T}(\boldsymbol{x}) \quad \boldsymbol{\phi}|_{\boldsymbol{y}=\boldsymbol{g}(\boldsymbol{x})}\Big)^T \| = \infty \tag{1.29}$$

It is shown in [258], that (1.28) is satisfied if the number of independent measurements is greater than n_q. In other words, the number of independent measurements should be enough to decouple completely the unknown input vector $\boldsymbol{d}$ which is a quite classical result in the analytical elimination theory.

The dynamical state equation of the decoupled system is then given by

$$\dot{\boldsymbol{z}}(t) = \frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}} \left(\boldsymbol{h}(\boldsymbol{x},\boldsymbol{u}) + \boldsymbol{K}(\boldsymbol{x},\boldsymbol{u})\boldsymbol{f}(t)\right)\Big|_{\boldsymbol{x}=\boldsymbol{\psi}_0(\boldsymbol{z},\bar{\boldsymbol{y}})} \tag{1.30}$$

Moreover, in order to guarantee that all faults affecting the system are also reflected by the decoupled state, the following condition must be fulfilled

$$\operatorname{rank}\left(\frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}}\boldsymbol{K}(\boldsymbol{x},\boldsymbol{u})\right) = \operatorname{rank}\left(\boldsymbol{K}(\boldsymbol{x},\boldsymbol{u})\right) \tag{1.31}$$

The structure of a nonlinear UIO for FDI then is given by

$$\begin{cases} \dot{\hat{\boldsymbol{z}}}(t) = \dfrac{\partial \hat{\boldsymbol{z}}}{\partial \boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}})}\boldsymbol{h}(\boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}}),\boldsymbol{u}) + \boldsymbol{H}\boldsymbol{R}(\hat{\boldsymbol{z}},\boldsymbol{y}) \\ \boldsymbol{r}(t) = \boldsymbol{R}(\hat{\boldsymbol{z}},\boldsymbol{y}) \end{cases} \tag{1.32}$$

under the assumption that a relation $\boldsymbol{R}(\boldsymbol{z},\boldsymbol{y}) = \boldsymbol{0}$ exists. In (1.32), $\boldsymbol{r}$ is the residual vector.

Now, the remaining problem is to design a the observer gain matrix $\boldsymbol{H}$, in such a way that the equilibrium point $\boldsymbol{e} = \boldsymbol{0}$ of the differential equation governing the estimation error $\boldsymbol{e} = \hat{\boldsymbol{z}} - \boldsymbol{z}$ is asymptotically stable. [258] proposes to design $\boldsymbol{H}$, such that the observer is locally stable (around $\boldsymbol{e} = \boldsymbol{0}$). To proceed, let us observe that

$$\begin{aligned} \dot{\boldsymbol{e}}(t) = \dot{\hat{\boldsymbol{z}}}(t) - \dot{\boldsymbol{z}}(t) = \frac{\partial \boldsymbol{T}(\hat{\boldsymbol{x}})}{\partial \hat{\boldsymbol{x}}}h(\hat{\boldsymbol{x}},\boldsymbol{u}) - \frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}}\boldsymbol{h}(\boldsymbol{x},\boldsymbol{u}) + \boldsymbol{H}\boldsymbol{R}(\hat{\boldsymbol{z}},\boldsymbol{y}) - \\ - \frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}}\boldsymbol{K}(\boldsymbol{x},\boldsymbol{u})\boldsymbol{f}(t)\Big|_{\boldsymbol{x}=\boldsymbol{\psi}_0(\boldsymbol{z},\bar{\boldsymbol{y}}),\hat{\boldsymbol{x}}=\boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}})} \end{aligned} \tag{1.33}$$

Denoting

$$\boldsymbol{\rho}(\boldsymbol{e},t) = \frac{\partial \boldsymbol{T}(\hat{\boldsymbol{x}})}{\partial \hat{\boldsymbol{x}}}\boldsymbol{h}(\hat{\boldsymbol{x}},\boldsymbol{u}) - \frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}}\boldsymbol{h}(\boldsymbol{x},\boldsymbol{u}) + \boldsymbol{H}\boldsymbol{R}(\hat{\boldsymbol{z}},\boldsymbol{y})\Big|_{\boldsymbol{x}=\boldsymbol{\psi}_0(\boldsymbol{z},\bar{\boldsymbol{y}}),\hat{\boldsymbol{x}}=\boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}})} \tag{1.34}$$

equation (1.33) can be written

$$\dot{\boldsymbol{e}}(t) = \boldsymbol{\rho}(\boldsymbol{e},t) - \frac{\partial \boldsymbol{T}(\boldsymbol{x})}{\partial \boldsymbol{x}}\boldsymbol{K}(\boldsymbol{x},\boldsymbol{u})\boldsymbol{f}(t)\Big|_{\boldsymbol{x}=\boldsymbol{\psi}_0(\boldsymbol{z},\bar{\boldsymbol{y}})} \tag{1.35}$$

Then, under the assumption of a fault-free system ($\boldsymbol{f} = \boldsymbol{0}$), a first-order Taylor expansion of (1.35) around $\boldsymbol{e} = \boldsymbol{0}$ gives

$$\dot{\boldsymbol{e}}(t) \approx \boldsymbol{F}(t)\boldsymbol{e} \tag{1.36}$$

with

$$\boldsymbol{F}(t) = \frac{\partial}{\partial \boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}})}\left(\frac{\partial T(\hat{\boldsymbol{x}})}{\partial \hat{\boldsymbol{x}}}\boldsymbol{h}(\hat{\boldsymbol{x}},\boldsymbol{u})\right)\frac{\partial \boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}})}{\partial \hat{\boldsymbol{z}}} + \boldsymbol{H}(\hat{\boldsymbol{x}},\boldsymbol{u})\frac{\partial \boldsymbol{R}(\hat{\boldsymbol{z}},\boldsymbol{y})}{\partial \hat{\boldsymbol{z}}}|_{\hat{\boldsymbol{x}}=\boldsymbol{\psi}_0(\hat{\boldsymbol{z}},\bar{\boldsymbol{y}})} \tag{1.37}$$

Thus, the solution consists in choosing $\boldsymbol{H}(\hat{\boldsymbol{x}},\boldsymbol{u})$ so that the time-varying system (1.36) is stable.

Another solution consists in choosing $\boldsymbol{F}$ constant, so that, the real part of its eigenvalues are strictly negative and in deducing $\boldsymbol{H}(\hat{\boldsymbol{x}},\boldsymbol{u})$ from (1.37). This solution allows to adequately manage the dynamics of the nonlinear UIO, which is an important aspect from FDI viewpoint.

An alternative to these solutions is also proposed in [125]. Under the assumptions rank$\frac{\partial \boldsymbol{y}(\boldsymbol{x})}{\partial \boldsymbol{x}} = n_x$ and $\lim_{\|\boldsymbol{x}\|\to\infty} \|\boldsymbol{y}(\boldsymbol{x})\| = \infty$ and additionally some Lipschitz conditions, sufficient conditions for the stability of the nonlinear UIO (1.32) are proposed. A design algorithm based on Linear Matrix Inequality (LMI) is proposed and FDI performance specifications are also handled in the design procedure using the concept of LMI regions.

Remark 1.5. *The work reported in [43] addresses the particular class of nonlinear systems that are described by*

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{\Phi}(\boldsymbol{x}) + \boldsymbol{E}\boldsymbol{d}(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{1.38}$$

where the nonlinear function $\boldsymbol{\Phi}(\boldsymbol{x})$ verifies the Lipschitz condition. A full order nonlinear UIO is proposed by the authors and a sufficient condition for its existence is provided in terms of a LMI problem. It is shown than the established condition is also necessary when applied to linear systems (i.e., $\boldsymbol{\Phi}(\boldsymbol{x}) = \boldsymbol{0}$) and the proposed method becomes the classical ones of linear UIOs, see for instance [55, 142]. This theory is not presented here since it is used and improved in Chapter 4.

- **Application to the Mars Express Spacecraft**

In [233, 234], the UIO approach is used for thruster fault diagnosis of the Mars Express (MEX) spacecraft subject to disturbance, uncertainty and measurement noises. The main challenge is the detection and the isolation of faults in any one of the four active thrusters of the spacecraft during the phases of main engine burn that cause large torque and centre of mass disturbances. This is the so-called "thruster modulation" problem, which is difficult to solve using classical robust FDI methods. The structure of the MEX orbiter consists of a cube-shaped spacecraft together with two solar panel "wings" (see Fig. 1.4 for illustration).

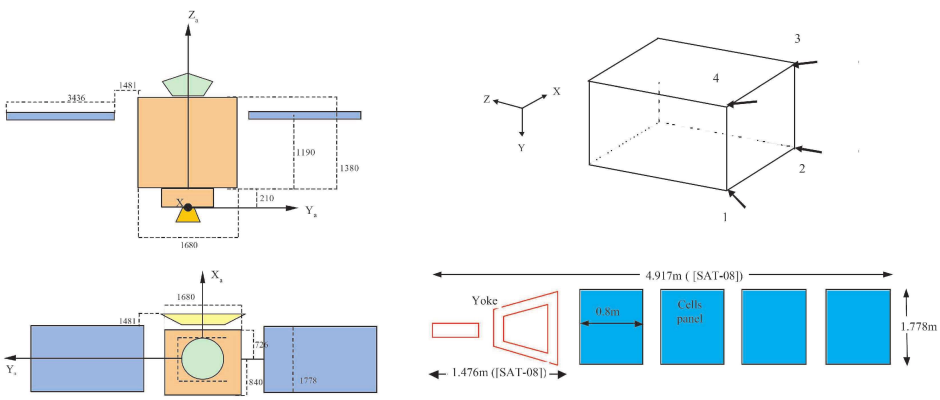


Figure 1.4 – MEX spacecraft structure [234]

The proposed FDI strategy is based on a bank of UIOs (see Section 1.3.6) with minimum variance state estimation error, where a separate estimation of disturbance torque makes the isolation possible. Each observer is designed to be sensitive to a subset of faults (that have to be detected and isolated). The unknown input directions are estimated via additional states in an augmented state observer structure [39]. Instead of using the nonlinear model of the spacecraft, a local linear mathematical models are estimated by means of a robust dynamic system identification approach based on the minimisation of the estimation error [260]. The unknown inputs are updated in the moving window and the minimum variance estimator is

re-initialized at the end of each window period. It is assumed that faults do not occur during the unknown input estimation phase.

1.3.2.3 Eigenstructure Assignment

In a similar way to UIO approach, the Eigenstructure Assignment (EA) technique aims at decoupling the effects of unknown inputs from the residual $\boldsymbol{r}$. To the best knowledge of the author, only linear approaches have been developed. Therefore, consider a LTI system with faults and unknown inputs

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{E}_{f_1}\boldsymbol{f}(t) + \boldsymbol{E}\boldsymbol{d}(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{D}\boldsymbol{u}(t) + \boldsymbol{E}_{f_2}\boldsymbol{f}(t) \end{cases} \tag{1.39}$$

where $\boldsymbol{E}_{f_1}$ and $\boldsymbol{E}_{f_2}$ are entry (fault distribution) matrices multiplying the fault vector $\boldsymbol{f} \in \mathbb{R}^{n_f}$, $\boldsymbol{d}(t) \in \mathbb{R}^{n_d}$ is the unknown input (or disturbance) vector entering the system through the known distribution matrix $\boldsymbol{E}$ assumed to be full column rank. Matrices $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ and $\boldsymbol{D}$ are of appropriate dimensions and $(\boldsymbol{A}, \boldsymbol{C})$ is assumed to be an observable pair.

Considering the above system, a Luenberger-like full state observer [182]

$$\begin{cases} \dot{\hat{\boldsymbol{x}}}(t) = \boldsymbol{A}\hat{\boldsymbol{x}}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{L}\left(\boldsymbol{y}(t) - \hat{\boldsymbol{y}}(t)\right) \\ \hat{\boldsymbol{y}}(t) = \boldsymbol{C}\hat{\boldsymbol{x}}(t) + \boldsymbol{D}\boldsymbol{u}(t) \end{cases} \tag{1.40}$$

can be built to create a residual generator vector $\boldsymbol{r} \in \mathbb{R}^{n_r}$ defined according to the relation

$$\boldsymbol{r}(t) = \boldsymbol{Q}\left(\boldsymbol{y}(t) - \hat{\boldsymbol{y}}(t)\right) \tag{1.41}$$

where $\hat{\boldsymbol{x}}(t) \in \mathbb{R}^{n_x}$ is the state estimate vector, $\hat{\boldsymbol{y}}(t) \in \mathbb{R}^{n_y}$ is the output estimate vector, and $\boldsymbol{Q}$ is the residual weighting matrix.

Defining the state estimation error $\boldsymbol{e} = \boldsymbol{x} - \hat{\boldsymbol{x}}$, then the residual generator is governed by the following equations

$$\begin{cases} \dot{\boldsymbol{e}}(t) = \boldsymbol{A}_c\boldsymbol{e}(t) + \boldsymbol{E}\boldsymbol{d}(t) + \boldsymbol{E}_{f_1}\boldsymbol{f}(t) - \boldsymbol{L}\boldsymbol{E}_{f_2}\boldsymbol{f}(t) \\ \boldsymbol{r}(t) = \boldsymbol{H}\boldsymbol{e}(t) + \boldsymbol{Q}\boldsymbol{E}_{f_2}\boldsymbol{f}(t) \end{cases} \tag{1.42}$$

where $\boldsymbol{A}_c = (\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})$ and $\boldsymbol{H} = \boldsymbol{Q}\boldsymbol{C}$. The Laplace transformed residual response to faults and unknown inputs is thus

$$\boldsymbol{r}(s) = \boldsymbol{Q}\boldsymbol{E}_{f_2}\boldsymbol{f}(s) + \boldsymbol{H}(s\boldsymbol{I} - \boldsymbol{A}_c)^{-1}(\boldsymbol{E}_{f1} - \boldsymbol{L}\boldsymbol{E}_{f2})\boldsymbol{f}(s) + \boldsymbol{H}(s\boldsymbol{I} - \boldsymbol{A}_c)^{-1}\boldsymbol{E}\boldsymbol{d}(s) \tag{1.43}$$

There is a conflict between the effects that the uncertainty terms $\boldsymbol{E}\boldsymbol{d}$ and the fault terms $\boldsymbol{E}_{f_1}\boldsymbol{f}$ and $\boldsymbol{E}_{f_2}\boldsymbol{f}$ have on the residual response. In order to make the residual $\boldsymbol{r}$ be independent of unknown inputs $\boldsymbol{d}$, it is necessary to null the entries in the transfer function matrix between the residual and the unknown inputs, i.e.,

$$\boldsymbol{G}_{rd}(s) = \boldsymbol{Q}\boldsymbol{C}(s\boldsymbol{I} - \boldsymbol{A}_c)^{-1}\boldsymbol{E} = \boldsymbol{0} \tag{1.44}$$

Once $\boldsymbol{E}$ is known, the problem is to find the matrices $\boldsymbol{L}$ and $\boldsymbol{Q}$ to satisfy (1.44), in addition to choosing the suitable eigenvalues to optimize the FDI performances [169].

• Disturbance Decoupling Using Left Eigenvectors Assignment

Disturbance decoupling design via EA is to assign left observer eigenvectors orthogonal to all columns of $\boldsymbol{E}$. This method can be briefly summarized as follows:

- **Step 1:** Calculate the residual weighting matrix $\boldsymbol{Q}$ such that $\boldsymbol{QCE} = \boldsymbol{0}$
- **Step 2:** Determine the eigenstructure of $\boldsymbol{A}_c$: the eigenvalues of the observer are chosen according to the desired dynamic property of the residuals. The rows of $\boldsymbol{QC}$ must be the n_r left eigenvectors of $\boldsymbol{A}_c$. The remaining $(n_x - n_r)$ left eigenvectors will be chosen so that one can ensure a design with good conditioning.
- **Step 3:** Compute the gain matrix $\boldsymbol{L}$ using an appropriate EA technique.

A detailed design procedure for the disturbance decoupling residual generator via left eigenvector assignment is discussed in Chapter 3.

Remark 1.6. *The observer feedback EA problem can be handled by means of a transformation of the dual control form. On assignment of the right eigenvectors to the dual control problem, these eigenvectors become the left eigenvectors of the observer system [39, 169]. The assignment of the right eigenvectors for the control problem is a well-developed technique, see e.g., [168, 169, 177, 262].*

• Disturbance Decoupling Using Right Eigenvectors Assignment

If the left eigenvector assignability conditions are not satisfied, an alternative approach can be used is to assign the columns of the matrix $\boldsymbol{E}$ as right eigenvectors of the observer dynamics. This approach is given by the following theorem:

Theorem 1.2 (Patton and Frank [229])**.** *The sufficient conditions for satisfying the unknown input decoupling requirement (for right EA) are*

1. $\boldsymbol{QCE} = \boldsymbol{0}$,
2. *all the rows of the matrix* $\boldsymbol{E}$ *are right eigenvectors of* $\boldsymbol{A}_c$ *corresponding to any eigenvalues.*

The assignment of the right observer eigenvectors (left eigenvector of dual controller) is a relatively new problem, only few investigators have considered this problem [46, 225]. Some preliminaries to the assignment method proposed in [225] is presented in the following theorem.

Theorem 1.3 (Patton and Chen [225])**.** *A vector* $\boldsymbol{v}_i$ *can be assigned as a right eigenvector of* $\boldsymbol{A}_c$ *corresponding to eigenvalue* $\lambda_i \in \Lambda(\boldsymbol{A}_c)$ *only if "one" of the following necessary conditions is satisfied:*

1. $\boldsymbol{v}_i$ *is not the right eigenvector of* $\boldsymbol{A}$ *corresponding to* λ_i *and* $\boldsymbol{Cv}_i \neq \boldsymbol{0}$
2. $\boldsymbol{v}_i$ *is the right eigenvector of* $\boldsymbol{A}$ *corresponding to* λ_i *and* $\boldsymbol{Cv}_i = \boldsymbol{0}$.

For the right eigenvector $\boldsymbol{v}_i$ of $\boldsymbol{A}_c = (\boldsymbol{A} - \boldsymbol{LC})$, it is possible to write

$$(\boldsymbol{A} - \boldsymbol{LC})\boldsymbol{v}_i = \lambda_i \boldsymbol{v}_i \tag{1.45}$$

and this leads to

$$\boldsymbol{LCv}_i = (\boldsymbol{A} - \lambda_i \boldsymbol{I})\boldsymbol{v}_i \tag{1.46}$$

The assignment of $\boldsymbol{v}_i$ as the right eigenvector of $\boldsymbol{A}_c$ is to find the matrix $\boldsymbol{L}$ to satisfy (1.46). This equation has solutions only if either condition in Theorem 1.3 holds true.

Remark 1.7. *If the desired observer eigenstructure is assignable (using left or right eigenvectors), perfect decoupling can be achieved, otherwise the eigenvectors must be chosen to be close, in some norm sense, to the desired eigenvectors. In this situation, the residuals also have low sensitivity to uncertainties due to approximate decoupling*

Remark 1.8. *The term $\boldsymbol{Ed}$ in* (1.39) *can be used to describe the additive disturbance as well as a number of other different kinds of modelling uncertainties. Examples are: noise, non-linear terms in system dynamics, terms arise from time-varying system dynamics, linearization and model reduction errors, parameter variations. In the following, two examples in the representation of modelling errors as additive disturbance term $\boldsymbol{Ed}$ are given.*

Example 1: *Consider that the system dynamics with parameter perturbations is represented by*

$$\dot{\boldsymbol{x}}(t) = (\boldsymbol{A} + \Delta\boldsymbol{A})\boldsymbol{x}(t) + (\boldsymbol{B} + \Delta\boldsymbol{B})\boldsymbol{u}(t) \tag{1.47}$$

The parameter perturbations considered in the robust control field are often approximated by

$$\Delta\boldsymbol{A} \approx \sum_{i=1}^{n_a} \alpha_i(t)\boldsymbol{A}_i, \quad \Delta\boldsymbol{B} \approx \sum_{i=1}^{n_b} \beta_i(t)\boldsymbol{B}_i \tag{1.48}$$

where $\boldsymbol{A}_i$ and $\boldsymbol{B}_i$ are known matrices with proper dimensions and α_i and β_i are unknown scalar time-varying factors. In this case, the modelling errors can be approximated by

$$\boldsymbol{Ed}(t) = \Delta\boldsymbol{A}\boldsymbol{x}(t) + \Delta\boldsymbol{B}\boldsymbol{u}(t) = \begin{bmatrix}\boldsymbol{A}_1 & \dots & \boldsymbol{A}_{n_a}, & \boldsymbol{B}_1 & \dots & \boldsymbol{B}_{n_b}\end{bmatrix} \begin{bmatrix} \alpha_1(t)\boldsymbol{x}(t) \\ \vdots \\ \alpha_{n_a}(t)\boldsymbol{x}(t) \\ \beta_1(t)\boldsymbol{u}(t) \\ \vdots \\ \beta_{n_b}(t)\boldsymbol{u}(t) \end{bmatrix} \tag{1.49}$$

Example 2: *Consider the system matrices being functions of the parameter vector $\boldsymbol{\alpha} \in \mathbb{R}^{n_p}$, i.e.,*

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}(\boldsymbol{\alpha})\boldsymbol{x}(t) + \boldsymbol{B}(\boldsymbol{\alpha})\boldsymbol{u}(t) \tag{1.50}$$

If the parameter has a perturbation around a nominal condition $\boldsymbol{\alpha} = \boldsymbol{\alpha}_0$, this equation can be expanded as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}(\boldsymbol{\alpha}_0)\boldsymbol{x}(t) + \boldsymbol{B}(\boldsymbol{\alpha}_0)\boldsymbol{u}(t) + \sum_{i=1}^{n_p} \left\{ \frac{\partial \boldsymbol{A}}{\partial \boldsymbol{\alpha}_i}\delta\alpha_i\boldsymbol{x}(t) + \frac{\partial \boldsymbol{B}}{\partial \alpha_i}\delta\alpha_i\boldsymbol{u}(t) \right\} \tag{1.51}$$

In this case, the distribution matrix and unknown disturbance vector are expressed as

$$\boldsymbol{E} = \begin{bmatrix} \frac{\partial \boldsymbol{A}}{\partial \alpha_1} & \frac{\partial \boldsymbol{B}}{\partial \alpha_1} & \dots & \frac{\partial \boldsymbol{A}}{\partial \alpha_{n_p}} & \frac{\partial \boldsymbol{B}}{\partial \alpha_{n_p}} \end{bmatrix} \tag{1.52}$$

$$\boldsymbol{d}(t) = \begin{bmatrix} \delta\alpha_1\boldsymbol{x}^T(t) & \delta\alpha_1\boldsymbol{u}^T(t) & \dots & \delta\alpha_{n_p}\boldsymbol{x}^T(t) & \delta\alpha_{np}\boldsymbol{u}^T(t) \end{bmatrix} \tag{1.53}$$

A more detailed study of this problem can be found in [40, 226, 228].

1.3.2.4 Sliding Mode Observers

A special position among observer-based methods is occupied by the sliding mode observer (SMO). SMOs differ from linear Luenberger observers in that there is a nonlinear discontinuous term injected into the observer depending on the output estimation error. These observers are more robust than the Luenberger-like observers, as the discontinuous term enables the observer to reject disturbances, and also a class of mismatch between the system and the observer. The importance of the SMOs for FDI lies in their ability to reconstruct unmeasurable signals in a process, regardless of noise and uncertainty. SMOs force the output of the observer to exactly track the measured system output. SMOs have a natural fault estimation property [77] since the "equivalent output error injection" needs to replicate and cancel the fault effects so that the output estimation error is zero.

In the work of Hermans and Zarrop [138] a SMO was designed such that, in the presence of faults, the sliding motion is destroyed. Edwards et al. [77] used the same observer to estimate and thus detect and isolate faults using the so-called "equivalent output error injection" concept. However, in the presence of other disturbances (unmodelled dynamics, external disturbances, etc.), the estimation methods described in [77] are no longer accurate. Tan and Edwards [274] proposed a design method for the observer parameters such that the $\mathcal{L}_2$ gain from the disturbances to the fault estimation is minimised. Other techniques for designing FDI and FDD algorithms using SMOs can be found in [6].

The system model for the FDI analysis using SMO is based on a LTI system described by

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{E}_{f_a}\boldsymbol{f}_a(t,\boldsymbol{u}) + \boldsymbol{E}\boldsymbol{d}(t,\boldsymbol{y},\boldsymbol{u}) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{1.54}$$

where $\boldsymbol{d}(t,\boldsymbol{y},\boldsymbol{u}) \in \mathbb{R}^{n_d}$ represents the disturbance (uncertainty) signal. The matrix $\boldsymbol{E} \in \mathbb{R}^{n\times n_d}$ provides the disturbance structure. Actuator faults $\boldsymbol{f}_a(t,\boldsymbol{u}) \in \mathbb{R}^{n_{f_a}}$ are assumed to enter in the system through a distribution matrix $\boldsymbol{E}_{f_a} \in \mathbb{R}^{n\times n_{f_a}}$.

A sliding mode observer for actuator faults proposed by Tan and Edwards [274] has the structure

$$\begin{cases} \dot{\boldsymbol{z}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) - \boldsymbol{G}_l\boldsymbol{e}_y(t) + \boldsymbol{G}_n\boldsymbol{\nu}(t) \\ \boldsymbol{e}_y(t) = \boldsymbol{C}\boldsymbol{z}(t) - \boldsymbol{y}(t) \end{cases} \tag{1.55}$$

with a typical Luenberger gain matrix $\boldsymbol{G}_l$ and the addition of a gain $\boldsymbol{G}_n$ associated with the nonlinear injection term. The signal

$$\boldsymbol{\nu}(t) = -\rho_0(t,\boldsymbol{y},\boldsymbol{u})\mathrm{sign}(\boldsymbol{e}_y(t)) \tag{1.56}$$

is the "output error injection" signal which forces the state estimation error to reach the surface

$$\mathcal{S} = \{\boldsymbol{e} : \boldsymbol{C}\boldsymbol{e} = \boldsymbol{0}\}$$

in a finite time, and subsequently maintains the motion on this surface. The actuator fault reconstruction is defined as

$$\hat{\boldsymbol{f}}_a(t) = \boldsymbol{W}\boldsymbol{\nu}(t) \tag{1.57}$$

where the static gain $\boldsymbol{W} \in \mathbb{R}^{n_{f_a}\times n_m}$ must be selected by the designer.

A sensor fault problem can be posed and solved in a similar fashion. Consider a system subject

to sensor faults $\boldsymbol{f}_s \in \mathbb{R}^{n_{fs}}$ given by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{E}\boldsymbol{d}(t, \boldsymbol{y}, \boldsymbol{u}) \tag{1.58}$$

$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) + \boldsymbol{f}_s(t) \tag{1.59}$$

The sensor fault reconstruction can be posed in a similar fashion. The approach suggested in [274] is to transform the problem representation in (1.58) and (1.59) into the actuator formulation. This can be accomplished by first filtering the output

$$\dot{\boldsymbol{z}}_f(t) = -\boldsymbol{A}_f\boldsymbol{z}_f(t) + \boldsymbol{A}_f\boldsymbol{y}(t) \tag{1.60}$$

where $\boldsymbol{A}_f$ is a positive real matrix of time constants. Augmenting (1.58) with the filtering equation in (1.60) yields

$$\begin{cases} \begin{bmatrix} \dot{\boldsymbol{x}}(t) \\ \dot{\boldsymbol{z}}_f(t) \end{bmatrix} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{A}_f\boldsymbol{C} & -\boldsymbol{A}_f \end{bmatrix} \begin{bmatrix} \boldsymbol{x}(t) \\ \boldsymbol{z}_f(t) \end{bmatrix} + \begin{bmatrix} \boldsymbol{B} \\ \boldsymbol{0} \end{bmatrix} \boldsymbol{u}(t) + \begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{A}_f \end{bmatrix} \boldsymbol{f}_s(t) + \begin{bmatrix} \boldsymbol{E} \\ \boldsymbol{0} \end{bmatrix} \boldsymbol{d}(t) \\ \boldsymbol{y}_f = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{I} \end{bmatrix} \begin{bmatrix} \boldsymbol{x}(t) \\ \boldsymbol{z}_f(t) \end{bmatrix} \end{cases} \tag{1.61}$$

Now $\boldsymbol{f}_s$ appears as an actuator fault for the augmented system. Therefore, the observer structure for actuator faults in (1.55) can be used for the augmented system for sensor fault reconstruction.

In the further discussion on SMOs, only actuator faults are considered. If $\boldsymbol{E}_{f_a}$ from (1.54) has full column rank and $n_m \geq n_{f_a}$, then if $((\boldsymbol{A} - \boldsymbol{G}_l\boldsymbol{C}), \boldsymbol{E}_{f_a}, \boldsymbol{W}\boldsymbol{C})$ can be made passive[2] by choice of the gains $\boldsymbol{W}$ and $\boldsymbol{G}_l$, a sliding mode observer as described in (1.55)-(1.57) can be obtained so that the signal $\boldsymbol{z}$ estimates the unmeasurable states despite the presence of the fault. In (1.56) the gain $\rho_0(t, \boldsymbol{y}, \boldsymbol{u})$ must be sufficiently large to maintain a sliding motion in the presence of the faults and disturbances.

The observer synthesis is setup to produces a fault reconstruction signal $\hat{\boldsymbol{f}}$ that minimizes the effects of uncertainty and noise on the estimation error in an $\mathcal{L}_2$-gain fashion. The reconstruction signal in (1.57) can be designed such that, if $\boldsymbol{d} = 0$ then $\boldsymbol{e}_f = \boldsymbol{f} - \hat{\boldsymbol{f}}$ and the $\mathcal{L}_2$-gain from $\boldsymbol{d}$ to the estimation error $\boldsymbol{e}_f = \boldsymbol{f} - \hat{\boldsymbol{f}}$ is minimised. This is achieved by casting the problem of synthesizing the observer gains $\boldsymbol{G}_l$, $\boldsymbol{G}_n$ and $\boldsymbol{W}$ as a convex optimization problem using LMI software. Further details can be found in [274].

As in typical $\mathcal{L}_2$ minimisation problems, there are tradeoffs between robustness and performance as part of the design process. Obviously the observer can be designed to be robust against any uncertainty, but it can be over designed and the observers become insensitive to small magnitude and slow varying faults (and causes missed-alarms). However weighting the performance more over the robustness, can make the observer too sensitive to noise and uncertainty thus producing false alarms. Therefore careful tradeoffs between robustness and performance need to be made.

To summarize, the design procedure can be characterized by the following three steps:

- **Step 1:** Obtaining the model information $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$, including the uncertainty matrix $\boldsymbol{E}$

[2] This is the assumption made in [274] and can be understood as a requirement that $(\boldsymbol{A}, \boldsymbol{E}_{f_a}, \boldsymbol{C})$ is minimum phase and of relative degree one.

and the fault distribution $\boldsymbol{E}_{f_a}$.

- **Step 2:** Selecting the observer gains to guarantee the sliding surface is reached in finite time and that the motion when constrained to the surface is stable. This can be achieved by obtaining a SMO canonical form through state transformation, see e.g., [6, 77, 273, 274]. The observer gains $\boldsymbol{G}_l$ and $\boldsymbol{G}_n$ which minimize the effect of noise and uncertainty on the fault estimation is obtained using efficient LMI methods.

- **Step 3:** The fault signal reconstruction component is achieved through the gain $\boldsymbol{W}$ which is obtained as part of the LMI optimization process.

Remark 1.9. *From the isolation point of view, the above introduced SMO is somewhat different from other typical model based residual generation schemes. There are two types of estimation from the SMO; the state (or output) estimate and the fault reconstruction/estimate. The fault reconstruction signal tries to estimate the magnitude and the shape of the faults and it is therefore able to distinguish small and short term faults from any noise or uncertainty. Also fault isolation is inherent. If the fault estimates are "nonzero", faults are present, and the larger the fault estimation size, the more severe the faults. As shown in [3], in practice a small threshold is needed during a fault-free condition to allow for small variations, model mismatches and noise in the system.*

Remark 1.10. *It should also be noted, that there are sliding mode observer designs in the literature which deal directly with nonlinear systems. Although the design synthesis is much more challenging, for well understood nonlinear systems such as aircraft and spacecraft, these ideas can be applied directly.*

- **Application to the Mars Express Spacecraft**

A study presented in [5] is concerned with the development of an FDI scheme for the Mars Express Spacecraft (for more information see Section 1.3.2.2) operating in Sun Acquisition Mode (SACM). In this study a design of sliding mode observers for gyro and thruster fault detection and isolation is investigated. The main objective is to distinguish between the actuator and sensor faults which may occur during the SACM manoeuvre, and in the case of the later, to isolate the faulty gyro. A Monte Carlo campaign has been performed to assess the performance and the robustness of the SMO for the rigid satellite model with variations in initial conditions and parametric uncertainty. No effort were made to implement a threshold logic. In [201] this problem was further investigated and a fixed threshold was selected. The isolation task was achieved by a direction cosine vector projection method. A last square approach for an over-determined system was presented in [202] and used to detect fault in the gyros. A generalized bank of SMOs was used to isolate all possible sensor faults.

1.3.2.5 Geometric Approaches

The first concepts of geometric system theory were pioneered by Basile and Marro [9] and Wonham and Morse [299]. The concept was later extended to nonlinear systems where tools from differential geometry and Lie-algebra are primary used. In many cases, it is possible to convert the nonlinear and LTV problems into more easier LTI ones. The basic idea of the geometric approaches is to underline the problem of the residual generation for FDI with a given geometric interpretation.

The geometric approach to design detection filters was initiated by Massoumnia [190] for LTI systems. The geometric approach of the UIO problem was first introduced in [14] and different solutions were proposed in [94]. In particular, in Massoumnia [190] it was shown that the residual generation problem can be successfully solved for LTI system, using the geometric concept of unobservability subspaces. The concepts of invariant subspaces, separability and simultaneous detectability of the faults have been used for building a LPV FDI design procedure, see [23]. Related results in FDI filter design for LTV systems can be found in [74], for bilinear systems in [117] and the inversion-based approach for LTI systems in [75, 271].

Consider the state space description of the nominal LTI system subjected to multiple faults

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \sum_{i=0}^{n_f} \boldsymbol{R}_i f_i(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{1.62}$$

where $\boldsymbol{R}_i$ is the known fault direction vector via the unknown function f_i, representing the fault, enters. It is assumed that $(\boldsymbol{A}, \boldsymbol{C})$ is an observable pair. The goal is to detect and isolate faults by applying a residual generator based on the full-order state observer, as in (1.40) but with $\boldsymbol{D} = \boldsymbol{0}$.

Definition 1.1 (Edelmayer et al. [74])**.** A detection filter capable of detecting and isolating multiple faults is a state observer of the form as given in (1.40), whose static gain $\boldsymbol{L}$ is designed in such a way that the effects of the failure modes f_i are assigned to independent subspaces $\mathcal{W}_i \in \mathbb{R}^{n_x}$, different from zero. In geometrical terms

$$\mathrm{Im}\boldsymbol{R}_i \subseteq \mathcal{W}_i, \quad (\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})\mathcal{W}_i \subseteq \mathcal{W}_i, \quad i = 1, \ldots, n_f \tag{1.63}$$

such that

$$\mathrm{Im}\boldsymbol{R}_i \cap \mathrm{Ker}\boldsymbol{C} = 0 \tag{1.64}$$

Moreover, in the output error space, the output image of $\mathcal{W}_i$ is decoupled, i.e.,

$$\boldsymbol{C}\mathcal{W}_i \cap \sum_{i \neq j}^{n_f} \boldsymbol{C}\mathcal{W}_i = 0, \quad i, j = 1, \ldots, n_f \tag{1.65}$$

The closed loop transition matrix $(\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})$ is required to be stable, more precisely its eigenvalues $\lambda_i, i = 1, \ldots, n_x$ have all negative real parts assuming its egenvalue spectrum Λ is arbitrarily assignable with only conjugate symmetry constraints, i.e., $\max\{\Re(\lambda_i) : \lambda_i \in \Lambda(\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C}) < 0\}$, $\forall i = 1, \ldots, n_x$.

Relations (1.63)-(1.65) are respectively the detectability, input observability and output separability principles of the design. The subspaces $\mathcal{W}_i, i = 1, \ldots, n_f$ are called detection spaces of the filter. Relation (1.63) shows that $\mathcal{W}_i$ is $(\boldsymbol{C}, \boldsymbol{A})$-invariant subspace of the pair $(\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C}, \boldsymbol{R}_i)$. For practical reasons, it is important to use extremal $(\boldsymbol{C}, \boldsymbol{A})$-invariant subspaces in the design. It is advantageous to find the family of the smallest possible subspaces $\mathcal{W}_i$ satisfying the principles (1.63)-(1.65).

The $(\boldsymbol{C}, \boldsymbol{A})$-invariance property of $\mathcal{W}_i$ implies that the controllable space of $\boldsymbol{R}_i$ with respect to the closed-loop transition matrix $(\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})$ is the infimal $(\boldsymbol{C}, \boldsymbol{A})$-invariant subspace containing $\mathrm{Im}\boldsymbol{R}_i$, i.e., $\inf\langle \boldsymbol{A} - \boldsymbol{L}\boldsymbol{C} | \mathcal{R}_i \rangle$ [3]. This will be denoted by $\mathcal{W}_i^*(\mathcal{R}_i)$ in the sequel. That is to say,

[3] $\langle \boldsymbol{A} - \boldsymbol{L}\boldsymbol{C} | \mathcal{R}_i \rangle$ stands for the family of all $(\boldsymbol{A} - \boldsymbol{L}\boldsymbol{C})$-invariant subspaces bounded to the subspace $\mathcal{R}_i$.

the family of the controllable subspaces of $(\boldsymbol{A} - \boldsymbol{LC}|\boldsymbol{R}_i)$ is a subfamily of the $(\boldsymbol{C}, \boldsymbol{A})$-invariant subspaces of the filter.

Recall that the controllability subspace is the set $\mathcal{W}^* \subseteq \mathbb{R}^{n_x}$ of initial points $\boldsymbol{x}(0)$ that can be controlled by appropriate state feedback $\boldsymbol{K}$ to the origin of the state-space in finite time. $\mathcal{W}^*$ is always a linear subspace of $\mathbb{R}^{n_x}$. When $\mathcal{W}^* = \mathbb{R}^{n_x}$, the system is said to be controllable. More precisely, $\mathcal{W}_i^*$ is the controllable subspace of the pair $(\boldsymbol{A} - \boldsymbol{LC}|\boldsymbol{R}_i)$, i.e.,

$$\mathcal{W}_i^* = \langle \boldsymbol{A} - \boldsymbol{LC} | \mathrm{Im}\boldsymbol{R}_i \rangle \tag{1.66}$$

In order to compute the minimal $(\boldsymbol{C}, \boldsymbol{A})$-invariant subspaces a recursive algorithm can be used [298]

$$\mathcal{W}_i^{l+1} = \mathrm{Im}\boldsymbol{R}_i + \boldsymbol{A}(\mathcal{W}_i^l \cap \mathrm{Ker}\boldsymbol{C}), \quad \mathcal{W}_i^0 = 0 \tag{1.67}$$

and then the infimal subspace $\mathcal{W}_i^*$ is given by $\lim_{l \to \infty} \mathcal{W}_i^l$.

• Inversion-based Detection Filter Design

A view of the inversion-based input reconstruction, with special emphasis to the aspects of fault detection and isolation by using invariant subspaces, and the results of classical geometrical system theory is provided in the next. The power of this kind of geometric approach is due to its direct treatment of the fundamental structural questions at the root of many important synthesis problems in control and systems theory such as the properties of inverse generation.

The existence of a left inverse for an LTI system is introduced first.

Proposition 1.1 (Wonham [298])**.** *The system $\Sigma : (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ given in state space form is left invertible if and only if $\boldsymbol{A}$ is monic (i.e., it has full column rank) and*

$$\mathcal{V}^* \cap Im\boldsymbol{B} = 0 \tag{1.68}$$

where $\mathcal{V}^*$ is the supremal $(\boldsymbol{A}, \boldsymbol{B})$-invariant subspace in $\mathrm{Ker}\boldsymbol{B}$ and $\boldsymbol{F}$ is the feedback, such that $(\boldsymbol{A} - \boldsymbol{BF})\mathcal{V}^* \subseteq \mathcal{V}^*$ (i.e., $(\boldsymbol{A} - \boldsymbol{BF})$ is maximally unobservable).

This proposition, in particular, is equivalent to the condition that the largest controllability subspace of $\mathrm{Ker}\boldsymbol{C}$ (noted $\mathcal{X}^*$[4]) is zero. The subspace $\mathcal{V}^*$ can be calculated by using the $(\boldsymbol{A}, \boldsymbol{B})$-invariant subspace algorithm without explicitly constructing $\boldsymbol{F}$.

Proposition 1.2 (Edelmayer et al. [75])**.** *Consider the left invertible system $\Sigma : (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$. The dynamics of the (left) inverse can be given as the restriction of $(\boldsymbol{A} - \boldsymbol{BF})$ on $\mathcal{V}^*$,*

$$\boldsymbol{A}_{inv} = (\boldsymbol{A} - \boldsymbol{BF})|\mathcal{V}^* \tag{1.69}$$

The dimension of the state space for the inverse system is $n_{inv} = \dim\mathcal{V}^* = n_x - n_p(\boldsymbol{p})$, where n_x is the state dimension of Σ, $\boldsymbol{p}$ is its (vector) relative degree and $n_p(\boldsymbol{p}) = \sum_{i=1}^m p_i$.

LTI inversion design steps: the inverse dynamics of the system $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ can be obtained thanks to the algorithmic procedure described in the following.

[4]Note that, in the control literature, the controllability subspace is conventionally denoted by $\mathcal{R}$. The different notation is due to the possible mismatch with the subspace of the faults.

- **Step 1:** Calculate $\mathcal{V}^*$ by using the $(\boldsymbol{A}, \boldsymbol{B})$-invariant subspace algorithm [73]

- **Step 2:** Choose a basis for $\mathcal{V}^*$ and compute the state transformation matrix $\boldsymbol{T}$, i.e.,

$$\boldsymbol{z} = \boldsymbol{T}\boldsymbol{x} = \begin{bmatrix} \boldsymbol{\xi} \\ \boldsymbol{\eta} \end{bmatrix}, \qquad \boldsymbol{\xi} \in \mathcal{V}^{*\perp}, \;\; \boldsymbol{\eta} \in \mathcal{V}^* \tag{1.70}$$

such that

$$\boldsymbol{T}^{-1} = [\ \boldsymbol{B} \quad \boldsymbol{\Xi} \quad \boldsymbol{V}^*\ ], \quad \mathrm{Im}\boldsymbol{\Xi} \subset \mathcal{V}^{*\perp} \tag{1.71}$$

where $\boldsymbol{V}^*$ is the insertion map of $\mathcal{V}^*$. In a new coordinate system the state matrices will take the form

$$\bar{\boldsymbol{A}} = \begin{bmatrix} \bar{\boldsymbol{A}}_{11} & \bar{\boldsymbol{A}}_{12} \\ \bar{\boldsymbol{A}}_{21} & \bar{\boldsymbol{A}}_{22} \end{bmatrix}, \quad \bar{\boldsymbol{B}} = \begin{bmatrix} \bar{\boldsymbol{B}}_1 \\ \boldsymbol{0} \end{bmatrix}, \quad \bar{\boldsymbol{C}} = \begin{bmatrix} \bar{\boldsymbol{C}}_1 & \boldsymbol{0} \end{bmatrix} \tag{1.72}$$

Since $\bar{\boldsymbol{B}}_1$ is monic there exists a unique matrix $\boldsymbol{F}_2$ such that $\bar{\boldsymbol{B}}_1\boldsymbol{F}_2 = -\bar{\boldsymbol{A}}_{12}$.

- **Step 3:** Calculate the matrix $\boldsymbol{S} = [\bar{\boldsymbol{c}}_1^T, \ldots, (\bar{\boldsymbol{c}}_1\bar{\boldsymbol{A}}_{11}^{p_1-1})^T, \ldots, (\bar{\boldsymbol{c}}_m\bar{\boldsymbol{A}}_{11}^{p_m-1})^T]^T$

- **Step 4:** Introduce the vector of derivatives

$$\boldsymbol{v}_{inv}(t) = \begin{bmatrix} \boldsymbol{w}^T(t), & (y_1^{(p_1)}(t))^T, & \ldots, & (y_{n_y}^{p_m}(t))^T \end{bmatrix}^T \tag{1.73}$$

as the input of the inverse systems, where

$$\boldsymbol{w}(t) = \begin{bmatrix} y_1(t), & \ldots, & y_1^{(p_1-1)}(t), & \ldots, y_{n_y}(t), & \ldots, & y_{n_y}^{(p_m-1)}(t) \end{bmatrix}^T \tag{1.74}$$

Then, the dynamics of the inverse is obtained from

$$\dot{\boldsymbol{\eta}}(t) = \boldsymbol{A}_{inv}\boldsymbol{\eta}(t) + \boldsymbol{B}_{inv}\boldsymbol{v}_{inv}(t) \tag{1.75}$$

using the definitions

$$\boldsymbol{A}_{inv} = \bar{\boldsymbol{A}}_{22}, \quad \boldsymbol{B}_{inv} = \begin{bmatrix} \bar{\boldsymbol{A}}_{21}\boldsymbol{S}^{-1} \\ \boldsymbol{0} \end{bmatrix} \tag{1.76}$$

Finally, the input function $\boldsymbol{u}$ can be obtained from the following equation

$$\boldsymbol{u}(t) = \boldsymbol{C}_{inv}\boldsymbol{\eta}(t) + \boldsymbol{D}_{inv}\boldsymbol{v}_{inv}(t) \tag{1.77}$$

where $\boldsymbol{C}_{inv} = \boldsymbol{F}_2$, and

$$\boldsymbol{D}_{inv} = \boldsymbol{Z} - \begin{bmatrix} \boldsymbol{S}\bar{\boldsymbol{A}}_{11}\boldsymbol{S}^{-1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \tag{1.78}$$

The matrix $\boldsymbol{Z}$ is given by

$$\boldsymbol{Z} = \begin{bmatrix} \boldsymbol{Z}_1 & \boldsymbol{0} & \ldots & \boldsymbol{0} & \boldsymbol{E}_1 \\ \boldsymbol{0} & \boldsymbol{Z}_2 & \ldots & \boldsymbol{0} & \boldsymbol{E}_2 \\ \vdots & & \ddots & & \\ \boldsymbol{0} & \boldsymbol{0} & \ldots & \boldsymbol{Z}_{n_p} & \boldsymbol{E}_{n_p} \end{bmatrix}, \quad \boldsymbol{Z}_i = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix}, \quad \boldsymbol{E}_i = \begin{bmatrix} \boldsymbol{0} \\ \boldsymbol{e}_i^T \end{bmatrix}$$

where $\boldsymbol{e}_i$ being the ith unit vector in $\mathbb{R}^{n_p}$.

Remark 1.11. *In some situations the derivatives of certain output signals of the system are directly measured, and these can be utilized in this approach. This procedure can be used in some cases when other approaches like the* $(\boldsymbol{C}, \boldsymbol{A})$*-invariant subspace based detection filter design method fails to provide a stable filter. The cost at which it can be obtained is that one needs to use the integrals of certain output signals in the residual generators as artificial inputs.*

Remark 1.12. *The method described in this section considers linear geometric approaches. However nonlinear approaches have been also developed by some authors. The interested reader can refer to the non exhaustive list of publications [24, 57, 73, 75].*

1.3.3 Parameter Identification-based Approaches

To estimate the internal (states or physical parameters) and/or external (outputs) variables of the system, one is led to apply estimation or filtering techniques. Consider the dynamics of a nonlinear stochastic system expressed in the following state-space discrete time representation

$$\begin{cases} \boldsymbol{x}_k = \boldsymbol{f}_k(\boldsymbol{x}_{k-1}, \boldsymbol{u}_{k-1}) + \boldsymbol{w}_k \\ \boldsymbol{y}_k = \boldsymbol{g}_k(\boldsymbol{x}_k, \boldsymbol{u}_k) + \boldsymbol{v}_k \end{cases} \tag{1.79}$$

where $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ are independent zero-mean white noise sequences. The vector $\boldsymbol{x}_k \in \mathbb{R}^{n_x}$, $\boldsymbol{u}_k \in \mathbb{R}^{n_u}$ and $\boldsymbol{y}_k \in \mathbb{R}^{n_y}$ denotes the state, input and output vector, respectively. The vector function $\boldsymbol{f}_k$ and $\boldsymbol{g}_k$ describes the trajectory dynamic of the state and the output vector, respectively. Both $\boldsymbol{f}_k$ and $\boldsymbol{g}_k$ are assumed to be continuous and differentiable functions.

In general, considering the fault detection problem, the results of the estimation procedure can be used in two different ways:

- If one looks at the estimated outputs, the approach would be to form residual signals defined by the difference between the real measurements and the estimated output vector. Then performing various tests on the resulting innovation sequence, which can be used for hypothesis testing [70]. The decision test may be a simple threshold logic, or a more complex mechanism if the probabilities of wrong decisions are *a priori* imposed. Commonly used statistical test are the sequential Wald's test or the Pearson's test [10, 12].

- If one is interested in monitoring of the internal variables (states and/or physical parameters), a consistency check in the parameter or state space can be done in order to monitor (detect) the unusual changes in the system behavior. A geometric solution to derive a CR2 decision test can be found in [318].

Basically, an estimation problem rests in stochastic estimation of the state vector $\boldsymbol{x}_k$ via its *a-posteriori* probability density $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:k})$, where $\boldsymbol{Y}_{1:k} = \{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_k\}$ is a matrix containing the past measurements collected on the system and available at time k. According to the Bayes' theorem, the *a-posteriori* density $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:k})$ can be evaluated using the following recursion

$$p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:k}) = \frac{p(\boldsymbol{y}_k|\boldsymbol{x}_k)p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)})}{p(\boldsymbol{y}_k|\boldsymbol{Y}_{1:(k-1)})} \tag{1.80}$$

where $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)})$ is obtained using the Chapman-Kolmogorov's relation [167, 221]

$$p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)}) = \int p(\boldsymbol{x}_k|\boldsymbol{x}_{k-1})p(\boldsymbol{x}_{k-1}|\boldsymbol{Y}_{1:(k-1)})d\boldsymbol{x}_{k-1} \tag{1.81}$$

and $p(\boldsymbol{y}_k|\boldsymbol{Y}_{1:(k-1)})$ is a normalization constant defined by

$$p(\boldsymbol{y}_k|\boldsymbol{Y}_{1:(k-1)}) = \int p(\boldsymbol{y}_k|\boldsymbol{x}_k)p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)})d\boldsymbol{x}_k \tag{1.82}$$

Solving the recursive relation (1.81) provides an optimum solution to the filtration problem in the Bayesian sense [175].

Generally, the optimal estimation of (1.81) in finite time horizon is practically not possible [167, 175]. Solving this problem leads to different approximation techniques. Some of them will be introduced in the following paragraphs.

Remark 1.13. *Note that if the functions $\boldsymbol{f}$ and $\boldsymbol{g}$ are linear, and ones is interested in the estimation of an augmented state vector (including some physical parameters), then the filtering problem is naturally nonlinear due to the coupling between the states and the parameters.*

1.3.3.1 Extended Kalman Filter

An approach commonly used to solve the estimation problem given by (1.81) rests in using the Extended Kalman Filter (EKF). This approach is based on linearization of $\boldsymbol{f}$ and $\boldsymbol{g}$ using the first-order Taylor expansion around the current estimate of $\hat{\boldsymbol{x}}_{k|k}$ [50, 208].

The EKF estimation algorithm is based on the discrete time nonlinear state-space representation given by (1.79), where $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ are the uncorrelated process and measurement noise, respectively, that are assumed to be white Gaussian random processes with zero mean $E\{\boldsymbol{w}_k\} = \boldsymbol{0}$, $E\{\boldsymbol{v}_k\} = \boldsymbol{0}$ and with covariance matrix

$$E\left\{\begin{bmatrix} \boldsymbol{w}_i \\ \boldsymbol{v}_i \end{bmatrix}\begin{bmatrix} \boldsymbol{w}_j^T & \boldsymbol{v}_j^T \end{bmatrix}\right\} = \begin{bmatrix} \boldsymbol{Q} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R} \end{bmatrix}\delta_{ij}$$

$$E\{\boldsymbol{x}_0\} = \bar{\boldsymbol{x}}_0, \quad E\left\{(\boldsymbol{x}_0 - \boldsymbol{m}_0)(\boldsymbol{x}_0 - \boldsymbol{m}_0)^T\right\} = \boldsymbol{P}_0$$

where $\boldsymbol{x}_0$ is a stochastic state vector with mean $\bar{\boldsymbol{x}}_0$ and covariance matrix $\boldsymbol{P}_0$ uncorrelated with the state noise $\boldsymbol{w}_k$ and the measurement noise $\boldsymbol{v}_k$ vectors.

Following the method proposed in [208], the problem of recursively estimating the state vector $\boldsymbol{x}_k$ can be formulated as a nonlinear filtering problem that minimises the conditional mean-square error, i.e.,

$$\hat{\boldsymbol{x}}_k = \arg\min E\{\tilde{\boldsymbol{x}}_k\tilde{\boldsymbol{x}}_k^T|\boldsymbol{Y}_{1:k}\} \tag{1.83}$$

where $\tilde{\boldsymbol{x}}_k = \boldsymbol{x}_k - \hat{\boldsymbol{x}}_k$ is the state estimate error. The recursive algorithm of the extended Kalman filter is then given by the recursive application of the prediction-correction steps given by the following equations:

- **The prediction step**

$$\hat{\boldsymbol{x}}_{k|k-1} = \boldsymbol{f}_k(\hat{\boldsymbol{x}}_{k-1|k-1}, \boldsymbol{u}_k) \tag{1.84}$$

$$\boldsymbol{P}_{k|k-1} = \boldsymbol{A}_{k-1}\boldsymbol{P}_{k-1|k-1}\boldsymbol{A}_{k-1}^T + \boldsymbol{G}_{k-1}\boldsymbol{Q}\boldsymbol{G}_{k-1}^T \tag{1.85}$$

- **The correction step**

$$\boldsymbol{K}_k = \boldsymbol{P}_{k|k-1}\boldsymbol{C}_k^T(\boldsymbol{C}_k\boldsymbol{P}_{k|k-1}\boldsymbol{C}_k^T + \boldsymbol{H}_k\boldsymbol{R}\boldsymbol{H}_k^T)^{-1} \tag{1.86}$$

$$\hat{\boldsymbol{y}}_k = \boldsymbol{g}_k(\hat{\boldsymbol{x}}_{k|k-1}, \boldsymbol{u}_k) \tag{1.87}$$

$$\hat{\boldsymbol{x}}_{k|k} = \hat{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k(\boldsymbol{y}_k - \hat{\boldsymbol{y}}_k) \tag{1.88}$$

$$\boldsymbol{P}_k = (\boldsymbol{I} - \boldsymbol{K}_k\boldsymbol{C}_k)\boldsymbol{P}_{k|k-1} \tag{1.89}$$

where

$$\boldsymbol{A}_{k-1} = \frac{\partial \boldsymbol{f}}{\partial \boldsymbol{x}}(\hat{\boldsymbol{x}}_{k-1|k-1}), \quad \boldsymbol{C}_k = \frac{\partial \boldsymbol{g}}{\partial \boldsymbol{x}}(\hat{\boldsymbol{x}}_{k|k-1}), \quad \boldsymbol{G}_{k-1} = \frac{\partial \boldsymbol{f}}{\partial \boldsymbol{w}}(\boldsymbol{w}_{k-1}), \quad \boldsymbol{H}_k = \frac{\partial \boldsymbol{g}}{\partial \boldsymbol{v}}(\boldsymbol{v}_k)$$

characterize the system matrices, linearized and evaluated at the current value. Matrix $\boldsymbol{K}_k$ represents the non-stationary Kalman gain calculated at time instance k.

The main issue of this approach is the linearization process, which could lead to highly unstable filter performance if the time-step intervals are not sufficiently small. On the other hand, small time-step intervals could lead to computational overhead. One should also mention that the derivation of the Jacobian matrices are nontrivial in most practical cases and may lead to significant implementation burden. Some improved versions of the EKF were developed to avoid these drawbacks. Mentioned may be the Second-Order EKF (SOEKF) [252], which by calculating the Hessian matrix, can reduce the risk of divergence of the estimator, but against a larger computational cost. Another alternative is to use polynomial approximation techniques for nonlinear functions [208]. In comparison with the Taylor approximation, it does not require Jacobian calculations, but only function evaluations. This allows for an easier implementation.

Remark 1.14. *Although this method presents some optimality proofs, the key feature remains the a-priori choice of the covariance matrices* $\boldsymbol{Q}$ *and* $\boldsymbol{R}$*. The process covariance matrix* $\boldsymbol{Q}$ *controls the flexibility of the model whereas the measurement covariance matrix* $\boldsymbol{R}$ *controls the flexibility of the measurement equations.*

1.3.3.2 Particle Filtering

The particle filtering approach [65, 178, 242], also called the "Condensation Algorithm" or the "Markov Chain Monte Carlo Method" is a sequential probabilistic technique for approaching the distribution of the conditional probability of the state $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:k})$. The key idea is to represent (at any time instance k) the required posterior density function by a set of N random particles p^i, $i = 1, \ldots, N$ with associated weights and to compute estimates based on these samples and weights. At time instance k, each particle p^i is characterized by a pair $\{\boldsymbol{x}_k^i, \boldsymbol{w}_k^i\}_{i=1}^N$ (see Fig. 1.5 for illustration) where $\boldsymbol{x}_k^i$ represents the possible trajectory of the state (known as the *support points*) and $\boldsymbol{w}_k^i$ denotes the posterior density to this trajectory (*weights*). The particles evolve according to the state equation of the system (*prediction step*) and weights are adjusted at each iteration k depending on the observations (*correction step*).

Consider that the monitored system (1.79) is a Markov process[5], where $\boldsymbol{w}_k$ and $\boldsymbol{v}_k$ are the

[5] A Markov process is a stochastic process with the Markov property, where the distribution of future states depends only on the present state and not on how it arrived in the present state. It is distinguished from a Markov chain in that the states of a Markov process may be continuous as well as discrete.

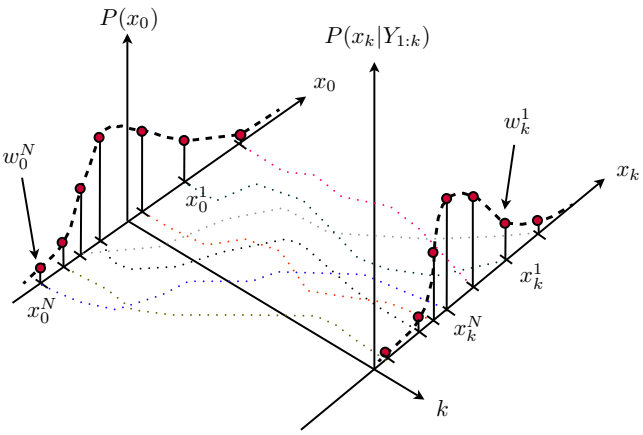


Figure 1.5 – Evolution of the conditional probability density

process and measurement noise, not necessary Gaussian. The weights are normalized such that $\sum_{i=1}^{N} \boldsymbol{w}_{k-1}^i = 1$. Then, the posterior density $p(\boldsymbol{x}_{k-1}|\boldsymbol{Y}_{1:(k-1)})$ at $k-1$ can be approximated as

$$p(\boldsymbol{x}_{k-1}|\boldsymbol{y}_{1:(k-1)}) \simeq \sum_{i=1}^{N} \boldsymbol{w}_{k-1}^i \delta(\boldsymbol{x}_{k-1} - \boldsymbol{x}_{k-1}^i) \tag{1.90}$$

where $\delta(\cdot)$ represents the Dirac delta measure. The recursive prediction-correction algorithm can be summarized as follows (the interested reader can refer [66]):

- **The prediction step**

If $p(\boldsymbol{x}_k, \boldsymbol{x}_{k-1}|\boldsymbol{Y}_{1:(k-1)})$ is the joint Probability Density Function (PDF) of the state, then the marginal PDF of the state $\boldsymbol{x}_k$ can be written as follows

$$p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)}) = \int p(\boldsymbol{x}_k, \boldsymbol{x}_{k-1}|\boldsymbol{Y}_{1:(k-1)}) d\boldsymbol{x}_{k-1} \tag{1.91}$$

According to the rule $p(x, y) = p(x|y)p(y)$ and taking up the assumption that the monitored system is described by a Markov process, it follows that $p(\boldsymbol{x}_k, \boldsymbol{x}_{k-1}|\boldsymbol{Y}_{1:(k-1)}) = p(\boldsymbol{x}_k|\boldsymbol{x}_{k-1})$ which makes it possible to reformulate the joint PDF (1.91) as follows

$$p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)}) = \int p(\boldsymbol{x}_k|\boldsymbol{x}_{k-1}) p(\boldsymbol{x}_{k-1}|\boldsymbol{Y}_{1:(k-1)}) d\boldsymbol{x}_{k-1} \tag{1.92}$$

Using the approximation given by equation (1.90), the above equation can be rewritten as follows

$$p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)}) = \sum_{i=1}^{N} \boldsymbol{w}_{k-1}^i p(\boldsymbol{x}_k|\boldsymbol{x}_{k-1}^i) \tag{1.93}$$

and makes it possible to write the predicted PDF $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)})$ according to the following relation

$$p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)}) = \sum_{i=1}^{N} \boldsymbol{w}_{k|k-1}^i \delta(\boldsymbol{x}_k - \boldsymbol{x}_{k|k-1}^i) \tag{1.94}$$

where $\boldsymbol{x}_{k|k-1}^i$ is obtained from independent realizations of the transition probability law $p(\boldsymbol{x}_k|\boldsymbol{x}_{k|k-1}^i)$ where $\boldsymbol{w}_{k|k-1}^i = \boldsymbol{w}_{k-1}^i$.

- **The correction step**

Consists in passing the predicted PDF law $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)})$ with the conditional PDF law $p(\boldsymbol{x}_k|\boldsymbol{Y}_{i:k})$ by use of the likelihood $p(\boldsymbol{y}_k|\boldsymbol{x}_k, \boldsymbol{Y}_{1:k})$. The conditional PDF can be then approximated by another Dirac delta support $\boldsymbol{x}_k^i = \boldsymbol{x}_{k|k-1}^i$ such that

$$p(\boldsymbol{x}_k|\boldsymbol{y}_{1:k}) = \sum_{i=1}^{N} \boldsymbol{w}_k^i \delta(\boldsymbol{x}_k - \boldsymbol{x}_k^i) \tag{1.95}$$

$$\boldsymbol{w}_k^i = \frac{\boldsymbol{w}_{k|k-1}^i p(\boldsymbol{y}_k|\boldsymbol{x}_k, \boldsymbol{Y}_{1:k})}{\sum_{i=1}^{N} \boldsymbol{x}_{k|k-1}^i p(\boldsymbol{y}_k|\boldsymbol{x}_k, \boldsymbol{Y}_{1:k})}, \quad i = 1, 2, \ldots, N \tag{1.96}$$

Remark 1.15. *However, the EKF always approximates $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k-1)})$ to be Gaussian. If the true density is non-Gaussian, then a Gaussian can never describe it well. In such cases, particle filters*[6] *will yield an improvement in performance in comparison to that of an EKF [8].*

1.3.3.3 Unscented Kalman Filter

The Unscented Kalman Filter (UKF) represents a derivative-free alternative to the EKF (discussed in the previous Section 1.3.3.1), and provides superior performance with an equivalent computational complexity [124, 288]. The state distribution is again represented by Gaussian random variables, but is now specified using a minimal set of careful chosen sample points. The sample points completely capture the true mean and covariance of the Gaussian distribution, and when propagated through the true nonlinear system, captures the posterior mean and covariance accurately to the 2nd order (Taylor series expansion) for any nonlinearity. This property is achieved by the *unscented transformation.* The idea is then to approximate the *a-posteriori* PDF $p(\boldsymbol{x}_k|\boldsymbol{Y}_{1:(k)})$ by a set of $(2n+1)$ points, called "sigma points", chosen so that some of their statistical properties (e.g., mean, covariance, etc.) are identical to those of the *a-priori* distribution. These points are then propagated through the system dynamics, through the analytical expressions of $\boldsymbol{f}$ and $\boldsymbol{g}$ given by (1.79), in order to evaluate the mean and the covariance matrix of the predicted state. The algorithm of the unscented transformation is introduced in [288].

Remark 1.16. *It should be noted that this transformation is very similar to the Monte Carlo used as part of the particle filtering. The main difference lies in the fact that the Sigma Points (particles in the case of particle filtering) are not random, but deterministically chosen in order to estimate the distribution of the state with a minimum number of points.*

Based on the unscented transformation and considering the random variable $\boldsymbol{x}_k^a \in \mathbb{R}^\eta$ defined as the concatenation of the state vector $\boldsymbol{x}_k$, of the process noise $\boldsymbol{w}_k$ and of the measurement

[6] A number of different types of particle filters exists in the literature, for a more details see [8]

noise $\boldsymbol{v}_k$, i.e., $\boldsymbol{x}_k^a = [\boldsymbol{x}_k^T, \boldsymbol{w}_k^T, \boldsymbol{v}_k^T]^T$ where $\eta = (2n + m)$, it follows that the unscented Kalman filter can be described as the recursive form of the unscented transformation obtained through the correction equation of the Kalman gain [158].

Considering the initial mean and covariance matrix of $\boldsymbol{x}_k^a$ as

$$\bar{\boldsymbol{x}}_0^a = E\left\{\boldsymbol{x}_0^a\right\} = [E\{\boldsymbol{x}_0\}, 0, 0]^T, \quad \boldsymbol{P}_0^a = E\left\{(\boldsymbol{x}_0^a - \bar{\boldsymbol{x}}_0^a)(\boldsymbol{x}_0^a - \bar{\boldsymbol{x}}_0^a)^T\right\} = \begin{bmatrix} \boldsymbol{P}_0 & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{Q} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{R} \end{bmatrix}$$

where the initial distribution of the Sigma points is given by

$$\boldsymbol{\chi}_{k-1}^{a,i} = \left[\ \bar{\boldsymbol{x}}_{k-1}^{a,i} \quad \bar{\boldsymbol{x}}_{k-1}^{a,i} \pm \sqrt{(\eta+\lambda)\boldsymbol{P}_{k-1}^{a,i}}\ \right], \qquad i = 1, \ldots, 2\eta \tag{1.97}$$

then the prediction-correction algorithm of the UKF is given by the following equations

- **The prediction step**

$$\boldsymbol{\chi}_{k|k-1}^i = \boldsymbol{f}_k(\boldsymbol{\chi}_{k-1}^i, \boldsymbol{u}_k) \tag{1.98}$$

$$\bar{\boldsymbol{x}}_{k|k-1} = \sum_{i=0}^{2\eta} \boldsymbol{w}_i^m \boldsymbol{\chi}_{k|k-1}^i \tag{1.99}$$

$$\boldsymbol{P}_{k|k-1} = \sum_{i=0}^{2\eta} \boldsymbol{w}_i^c [\boldsymbol{\chi}_{k|k-1}^i - \bar{\boldsymbol{x}}_{k|k-1}][\boldsymbol{\chi}_{k|k-1}^i - \bar{\boldsymbol{x}}_{k|k-1}]^T \tag{1.100}$$

$$\boldsymbol{y}_{k|k-1}^i = \boldsymbol{h}_k(\boldsymbol{\chi}_{k-1}^i, \boldsymbol{u}_k) \tag{1.101}$$

$$\bar{\boldsymbol{y}}_{k|k-1} = \sum_{i=0}^{2\eta} \boldsymbol{w}_i^m \boldsymbol{y}_{k|k-1}^i \tag{1.102}$$

- **The correction step**

$$\boldsymbol{P}_{\bar{y}_k\bar{y}_k} = \sum_{i=0}^{2\eta} \boldsymbol{w}_i^c [\boldsymbol{y}_{k|k-1}^i - \bar{\boldsymbol{y}}_{k|k-1}][\boldsymbol{y}_{k|k-1}^i - \bar{\boldsymbol{y}}_{k|k-1}]^T \tag{1.103}$$

$$\boldsymbol{P}_{\bar{x}_k\bar{y}_k} = \sum_{i=0}^{2\eta} \boldsymbol{w}_i^c [\boldsymbol{\chi}_{k|k-1}^i - \bar{\boldsymbol{x}}_{k|k-1}][\boldsymbol{y}_{k|k-1}^i - \bar{\boldsymbol{y}}_{k|k-1}]^T \tag{1.104}$$

$$\boldsymbol{K}_k = \boldsymbol{P}_{\bar{x}_k\bar{y}_k} \boldsymbol{P}_{\bar{y}_k\bar{y}_k}^{-1} \tag{1.105}$$

$$\bar{\boldsymbol{x}}_k = \bar{\boldsymbol{x}}_{k|k-1} + \boldsymbol{K}_k(\boldsymbol{y}_k - \bar{\boldsymbol{y}}_{k|k-1}) \tag{1.106}$$

$$\boldsymbol{P}_k = \boldsymbol{P}_{k|k-1} - \boldsymbol{K}_k \boldsymbol{P}_{\bar{y}_k\bar{y}_k} \boldsymbol{K}_k^T \tag{1.107}$$

The parameters $\boldsymbol{w}_i^m$ and $\boldsymbol{w}_i^c$ represent the weights associated with the Sigma points and are set through different parameter adjustment methods. These allow control the distribution of Sigma points around the mean and reflect the real distribution of the state (see [158] for more details).

- **Application to HL-20 Reusable Launch Vehicles**

The HL-20 Re-entry Launched Vehicle (RLV) (see Fig. 1.6 for an illustration) was defined as a component of the Personnel Launch System (PLS) mission. This has initially been designed to

support several manned-space missions including the orbital rescue of astronauts, the International Space Station (ISS) crew exchange and some satellite repair missions.

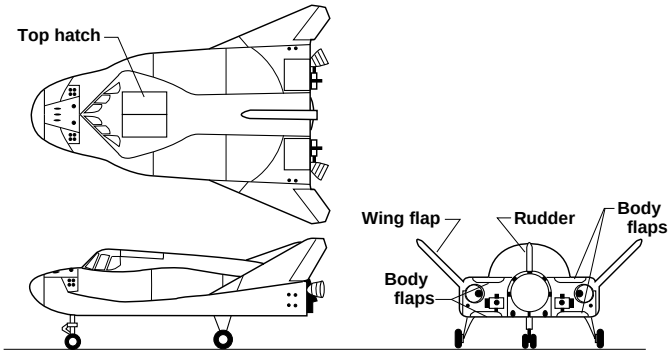


Figure 1.6 – The HL-20 RLV vehicle, ©1998 NASA

In the case of RLV, actuator faults and control effectors damages may lead to substantial performance degradation and instability of the closed-loop system. Information about the failed control surface position is necessary in order to access the remaining capabilities of the vehicle to be rotationally trimmed. Since no control surface sensors are today implemented on RLV (because of weight and thermal constraints), the faulty actuator deflection can be considered as an unknown input which has to be estimated. The work presented in [85] deals with this important issue. In this work, it is assumed that the faults in on the control surfaces have been successfully diagnosed (by any method) and thus the focus is on the fault identification problem. In order to estimate the position of the faulty actuator deflections, a nonlinear extended Kalman-type estimator is proposed. The identification scheme is based on a modified EKF which does not requires derivatives, leading to an easy implementation at each updating time. A Particle Swarm-based optimization algorithm is used to derive automatically the process and measurement noises matrices $\boldsymbol{Q}$ and $\boldsymbol{R}$.

1.3.4 Norm-based Approach

The robust residual generation problem can also be formulated as an optimization problem, where the sensitivity of the residuals with respect to noise and unknown disturbance is minimized and the sensitivity with respect to faults is maximized. A good survey paper of this approach can be found in [128, 187, 270].

1.3.4.1 The Pure H_∞ Filtering Formulation

The pure H_∞-based fault estimation problem is equivalent to the design problem of a (stable) dynamic filter $\boldsymbol{F}(s)$ such that, for all model perturbations $\Delta \in \|\Delta\|_\infty \leq 1$, $\hat{\boldsymbol{f}}$ is an optimal estimate, in the H_∞-norm sense, of the fault signal $\boldsymbol{f}$.

It is then shown in [205] that the problem of estimation of faults can be formulated by the synthesis scheme given in Fig. 1.7, where the transfer between the input signals $\boldsymbol{u}$, $\boldsymbol{d}$ and $\boldsymbol{f}$ to the output signal $\boldsymbol{y}$, can be written by the following Linear Fractional Representation (LFR)

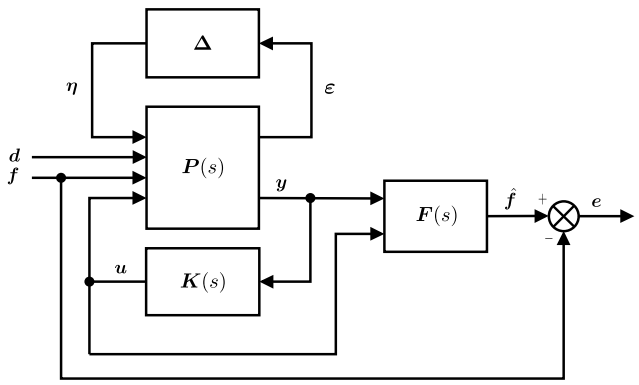


Figure 1.7 – The H_∞ fault estimation problem

form

$$\boldsymbol{y}(s) = \boldsymbol{F}_u(s)(\boldsymbol{P}(s), \boldsymbol{\Delta}(s)) \begin{pmatrix} \boldsymbol{d}(s) \\ \boldsymbol{f}(s) \\ \boldsymbol{u}(s) \end{pmatrix}, \quad \boldsymbol{u}(s) = \boldsymbol{K}(s)\boldsymbol{y}(s) \tag{1.108}$$

where $\boldsymbol{d}$ denotes the exogenous disturbances (including measurement noise) and $\boldsymbol{f}$ models the faults to be estimated. The controller is placed in a feedback control loop and is assumed to be known. The output of the filter $\boldsymbol{F}$ represents an estimate $\hat{\boldsymbol{f}}$ of the real fault signal $\boldsymbol{f}$. The filter $\boldsymbol{F}$ uses the all available signals $\boldsymbol{y}$ and $\boldsymbol{u}$ to construct the estimate signal $\hat{\boldsymbol{f}}$

$$\hat{\boldsymbol{f}}(s) = \boldsymbol{F}(s) \begin{pmatrix} \boldsymbol{y}(s) \\ \boldsymbol{u}(s) \end{pmatrix} \tag{1.109}$$

The known Linear Time-Invariant (LTI) model is denoted by $\boldsymbol{P}$. The block diagonal operator Δ specifies how the modelling errors influence the system.

To achieve high FDD performance, some model-based FDD schemes include a fault model in the design procedure. Then the design objectives, in terms of robustness and sensitivity, can be specified by a weighting filters $\boldsymbol{W}_f$ and $\boldsymbol{W}_d$ as

$$\tilde{\boldsymbol{f}}(s) = \boldsymbol{W}_f(s)\boldsymbol{f}(s), \quad \tilde{\boldsymbol{d}}(s) = \boldsymbol{W}_d(s)\boldsymbol{d}(s) \tag{1.110}$$

Here, the fault model is represented as a colouring filter for $\boldsymbol{f}$. In other words, $\boldsymbol{f}$ is considered to be the result of filtering a fictitious signal $\tilde{\boldsymbol{f}}$ through a filter $\boldsymbol{W}_f$. This filter is chosen taking into account the frequency location of the fault to be detected, e.g., if the energy of the faults to be detected are located at low frequencies, $\boldsymbol{W}_f$ is chosen to be a low-pass filter. The same assumptions hold for $\boldsymbol{d}$ and $\boldsymbol{W}_d$.

Now, let define the estimation error signal as $\boldsymbol{e} = \boldsymbol{f} - \hat{\boldsymbol{f}}$. Then the design problem turns out to be a minimization problem of the maximal gain of the closed-loop transfers from the signals $\tilde{\boldsymbol{f}}$ and $\tilde{\boldsymbol{d}}$ to the fault estimation error $\boldsymbol{e}$. In other words, the goal is to design the filter $\boldsymbol{F}$ so that

$$\|\boldsymbol{T}_{e\tilde{d}}\|_\infty < \alpha, \quad \forall \Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.111}$$

$$\|\boldsymbol{T}_{e\tilde{f}}\|_\infty < \beta, \quad \forall \Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.112}$$

where $\boldsymbol{T}_{e\tilde{f}}$ and $\boldsymbol{T}_{e\tilde{d}}$ denote the closed-loop transfer functions between $\boldsymbol{e}$ and $\tilde{\boldsymbol{f}}$, and between $\boldsymbol{e}$ and $\tilde{\boldsymbol{d}}$, respectively. α and β are two positive constants which are introduced to manage

separately $\|\boldsymbol{T}_{e\tilde{f}}\|_\infty$ and $\|\boldsymbol{T}_{e\tilde{d}}\|_\infty$.

Including the weighting filters $\boldsymbol{W}_f$ and $\boldsymbol{W}_d$ into the model $\boldsymbol{P}$ and using the small gain theorem, it is straightforward to verify that the conditions (1.111) and (1.112) are satisfied if and only if

$$\exists \boldsymbol{F} : \|\boldsymbol{F}_l(\tilde{\boldsymbol{P}}, \boldsymbol{F})\|_\infty < 1, \quad \forall \Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.113}$$

where $\boldsymbol{F}_l(\tilde{\boldsymbol{P}}, \boldsymbol{F})$ denotes the lower linear fractional transformation of $\tilde{\boldsymbol{P}}$ and $\boldsymbol{F}$. $\tilde{\boldsymbol{P}}$ is also deduced from $\boldsymbol{P}$, $\boldsymbol{W}_f$ and $\boldsymbol{W}_d$ by using tools of the LFR algebra.

The problem can by finally solved using two approaches developed in the research community. The first involves the solution of a Riccati equation (see for instance [186]) and the second approach uses linear matrix inequality (LMI) optimization techniques [315]. Since an LMI-based approach has the advantage of eliminating the regularity restrictions attached to the Riccati-based solution, the LMI-based approach is often preferred.

1.3.4.2 The H_∞/H_- Approach

The H_∞/H_- approach considers the problem of designing a structured residual vector $\boldsymbol{r}$ in the following general form

$$\boldsymbol{r}(s) = \boldsymbol{z}(s) - \hat{\boldsymbol{z}}(s) \tag{1.114}$$

This residual signal is the basis for FDI and should have desired properties. Let $\boldsymbol{y}$ be a subset of available measurements and $\boldsymbol{u}$ the control inputs, then $\boldsymbol{z}$ is defined as a linear combination of $\boldsymbol{y}$ and $\boldsymbol{u}$

$$\boldsymbol{z}(s) = \boldsymbol{M}_y \boldsymbol{y}(s) + \boldsymbol{M}_u \boldsymbol{u}(s) \tag{1.115}$$

where $\boldsymbol{M}_y$ and $\boldsymbol{M}_u$ are two residuals structuring (constant) matrices of appropriate dimension. They can also be called *FDD allocation* matrices.

The stable dynamical filter, $\boldsymbol{F}$, is supposed to generate

$$\hat{\boldsymbol{z}}(s) = \boldsymbol{F}(s) \begin{pmatrix} \boldsymbol{y}(s) \\ \boldsymbol{u}(s) \end{pmatrix}, \quad \boldsymbol{u}(s) = \boldsymbol{K}(s)\boldsymbol{y}(s) \tag{1.116}$$

where $\hat{\boldsymbol{z}}(s)$ is an estimation of $\boldsymbol{z}(s)$ and $\boldsymbol{K}$ denotes the controller.

This approach is based on jointly design of the FDD allocation matrices $\boldsymbol{M}_y$, $\boldsymbol{M}_u$ and the FDD filter $\boldsymbol{F}(s)$ such that the effects that faults have on the residual $\boldsymbol{r}$ are maximized in the H_- norm sense whilst the influence of the unknown inputs $\boldsymbol{d}$ and model uncertainties are minimized in the H_∞ norm sense. That is

$$\max \|\boldsymbol{T}_{rf}\|_-, \quad \text{and} \quad \min \|\boldsymbol{T}_{rd}\|_\infty, \ \forall \omega \in \Omega \tag{1.117}$$

where $\boldsymbol{T}_{rf}$ denotes the closed-loop transfer between $\boldsymbol{r}$ and $\boldsymbol{f}$, $\boldsymbol{T}_{rd}$ the closed-loop transfer between $\boldsymbol{r}$ and $\boldsymbol{d}$, and Ω is the frequency range where the energy of the faults is likely to be concentrated.

Various design goals and trade-offs can be achieved by using the different combinations of the norms. The main advantages are:

- H_∞ specifications are convenient to enforce robustness to model uncertainty (disturbances, parametric uncertainties, neglected dynamics),
- H_- specifications are useful for fault sensitivity requirements over specified frequency ranges,
- H_2 specifications are convenient to take into account the stochastic nature of disturbances, and
- H_{2g} specifications and poles assignment are convenient to tune the transient response and to enforce some minimum decay rate of the residuals.

The H_∞/H_- based FDD techniques are generally reputed to give robust but conservative solutions. The problem comes from the fact that, once the diagnostic filter is designed, no systematic analysis procedure is proposed to refine and manage the design trade-offs. It is clear that if the design method is associated with a suitable post-analysis process, an iterative refinement process can be established to get a good balance between different design trade-offs. In addition to get "as close as possible" to the required robustness/performance specifications, there is no reason for the final result to be conservative. Similarly to the H_∞ design and μ-analysis cycle used in the robust control community, the method proposed in [126, 128, 131, 132, 134] provides a solution to the aforementioned problems by providing a complete design/analysis cycle.

With regards to the design task, the procedure aims to generate a structured residual vector $\boldsymbol{r}$ in the general form (1.114)-(1.116). With regards to the post-design analysis procedure, a test is proposed to check if all the FDI objectives are achieved in the face of specified structured and/or unstructured model perturbations. The problem is formulated using an appropriate performance index, defined with respect to the effects of underlying faults on the residual signal. Testing the performances of residual generators results in a min-max optimization problem which cannot be formulated and solved using the classical "μ-analysis" framework. The method proposed by [131, 132, 134] provides a remarkably powerful solution to the problem by a FDI-oriented generalized μ-analysis procedure, denoted by the authors the μ_g-analysis procedure.

This method can be seen as a nice and practically "advanced" framework in which various design goals and trades-off are formulated and managed. It corresponds to a complete design/analysis cycle and has the following advantages:

- Systematic formulation of different design trade-offs.
- The residuals structuring matrices are jointly optimised with the dynamical part of the FDI filter. Their role is to merge optimally the available on-board measurements and the control signals to build the fault indicating signal.
- The control system can be included explicitly in the design.
- The μ_g tool is used as FDD-oriented performance measure: similarly to the μ-analysis procedure that allows for checking the robust performance of any LTI control law, the μ_g tool can be used as a general FDD-oriented performance measure for LTI model-based fault diagnosis scheme.

To go deeper into the method, consider the following model in the LFR form placed in a feedback

control loop (see Fig. 1.8).

$$\boldsymbol{y}(s) = (\Delta(s) * \boldsymbol{P}(s)) \begin{pmatrix} \boldsymbol{d}(s) \\ \boldsymbol{f}(s) \\ \boldsymbol{u}(s) \end{pmatrix}, \quad \boldsymbol{u}(s) = \boldsymbol{K}(s)\boldsymbol{y}(s) \tag{1.118}$$

The system model consists in a nominal LTI model $\boldsymbol{P}$ and a perturbation block $\Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1$ acting on the nominal model. $\underline{\Delta}$ describes the set of all perturbations of a prescribed structure, i.e.,

$$\underline{\Delta} = \{\text{blockdiag}(\delta_i^r I_{k_i}, \delta_j^c I_{k_{ji}}, \Delta_l)\} \tag{1.119}$$

where $\delta_i^r I_{k_i}, i = 1, \ldots, m_r$, $\delta_j^c I_{k_j}, i = 1, \ldots, m_c$ and $\Delta_l, l = 1, \ldots, m_c$ are known respectively as the "repeated real scalar" blocks, the "repeated complex scalar" blocks and the "full complex" blocks. It is assumed that all model perturbations are represented by Δ.

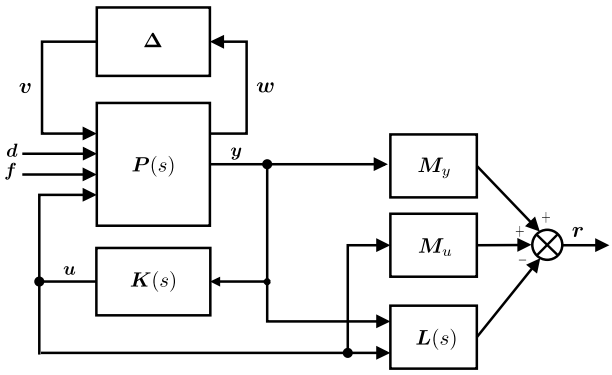


Figure 1.8 – The FDI filter design problem

Let $\boldsymbol{f}$ entering in $((\Delta(s) * \boldsymbol{P}(s)) * \boldsymbol{K})$ be detectable faults and the residual vector $\boldsymbol{r}$ be defined according to (1.114)-(1.116). The goal is to derive simultaneously $\boldsymbol{M}_y$, $\boldsymbol{M}_u$ and the state space matrices of the dynamical filter $\boldsymbol{L}$ such that the residual vector $\boldsymbol{r}$ meets the following specifications:

(S.1) - $\|\boldsymbol{T}_{rd}\|_\infty < \gamma_1$, for all perturbations model $\Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1$

(S.2) - $\|\boldsymbol{T}_{rf}\|_- > \gamma_2$, over a specified frequency range Ω for all $\Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1$

The specification (S.1) represents the worst-case robustness of the residual to disturbances $\boldsymbol{d}$ for all specified model perturbations, in the H_∞ norm sense. Under plant perturbation, the effect that the exogenous disturbances acting on the system have on the residual, can greatly increase. The fault detection performance may then be considerably degraded. A robust fault sensitivity specification is then needed to maintain a detection performance level of the FDI unit. Here the smallest gain of $\boldsymbol{T}_{rf}$ is used to guarantee the worst-case sensitivity of the residual to faults (see specification (S.2)). It is clear that the smaller γ_1 and the bigger γ_2 are, the better the fault detection performances will be.

Generally speaking, to achieve high FDI performances, model-based FDI schemes use disturbance, measurement noise and fault models into the design procedure. Here, such models are expressed in terms of shaping filters, i.e., of desired gain responses for the appropriate closed-loop transfers. The objectives are then turned into uniform bounds by means of the shaping filters. To proceed, let $\boldsymbol{W}_d$ and $\boldsymbol{W}_f$ be the (dynamical) shaping filters associated to the robustness and

fault sensitivity objectives defined such that

$$\|\boldsymbol{W}_d\|_\infty \leq \gamma_1, \qquad \|\boldsymbol{W}_f\|_- \geq \gamma_2 \tag{1.120}$$

Assume that $\boldsymbol{W}_d$ and $\boldsymbol{W}_f$ are invertible (this can be done without loss of generality because it is always possible to add zeros in $\boldsymbol{W}_d(s)$ and $\boldsymbol{W}_f(s)$ to make them invertible). Thus, it is obvious that if the condition

$$\|\boldsymbol{T}_{rd}\boldsymbol{W}_d^{-1}\|_\infty < 1, \quad \forall \Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.121}$$

is satisfied, then the robustness design specification (S.1) yields.

Now, the following proposition is needed to transform the fault sensitivity specification (S.2) into a H_∞ requirement.

Lemma 1.1 (Henry and Zolghadri [132])**.** *Consider the shaping filter $\boldsymbol{W}_f$ defined above. Let $\boldsymbol{W}_F$ be a right invertible transfer matrix so that $\|\boldsymbol{W}_f\|_- = \frac{\gamma_2}{\lambda}\|\boldsymbol{W}_F\|_-$ and $\|\boldsymbol{W}_F\|_- > \lambda$, where $\lambda = 1 + \gamma_2$. Define the signal $\tilde{\boldsymbol{r}}$ such that $\tilde{\boldsymbol{r}} = \boldsymbol{r} - \boldsymbol{W}_F(s)\boldsymbol{f}(s)$ (see Fig. 1.9 for easy reference). Then a sufficient condition for the fault sensitivity specification (S.2) to hold, is*

$$\|\boldsymbol{T}_{\tilde{r}f}\|_\infty < 1, \quad \forall \Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.122}$$

where $\boldsymbol{T}_{\tilde{r}f}$ denotes the transfer between $\tilde{\boldsymbol{r}}$ and $\boldsymbol{f}$

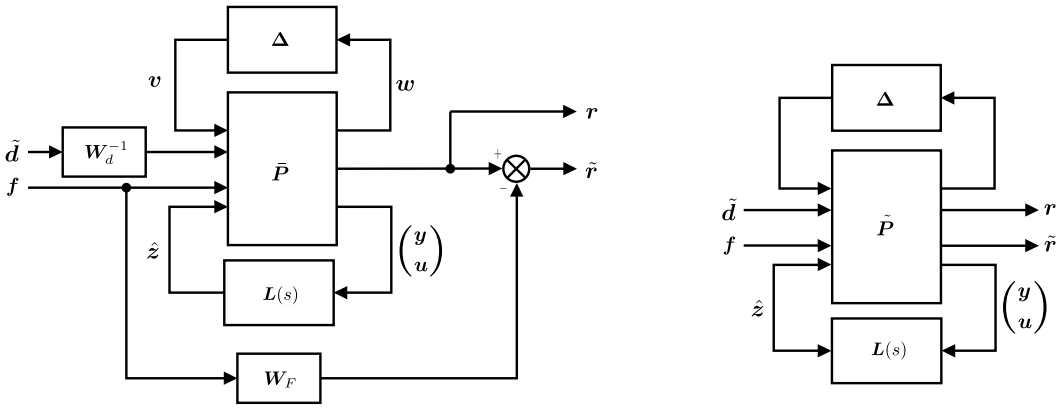


Figure 1.9 – The quasi standard setup for the design of a robust fault detection filter

Using the above lemma, the H_∞/H_- filter design problem can be re-casted in a fictitious H_∞ framework. Using linear fractional algebra and including γ_1, λ, $\boldsymbol{W}_F$, $\boldsymbol{W}_d$ and $\boldsymbol{K}$ into the model $\boldsymbol{P}$, one can derive from (1.118) a new model $\tilde{\boldsymbol{P}}\left(\boldsymbol{M}_y, \boldsymbol{M}_u\right)$ depending of the residual structuration matrices $\boldsymbol{M}_y$, $\boldsymbol{M}_u$ so that

$$\begin{pmatrix} \boldsymbol{r}(s) \\ \tilde{\boldsymbol{r}}(s) \end{pmatrix} = \left(\left(\Delta(s) * \tilde{\boldsymbol{P}}(\boldsymbol{M}_y, \boldsymbol{M}_u, s)\right) * \boldsymbol{L}(s)\right) \begin{pmatrix} \tilde{\boldsymbol{d}}(s) \\ \boldsymbol{f}(s) \end{pmatrix} \tag{1.123}$$

Then by virtue of the small gain theorem, it follows that a sufficient condition is

$$\|\tilde{\boldsymbol{P}}(\boldsymbol{M}_y, \boldsymbol{M}_u) * \boldsymbol{L}\|_\infty < 1 \tag{1.124}$$

This equation seems to be similar to a standard H_∞ equation. However, this is not the case

since the transfer $\tilde{\boldsymbol{P}}(\boldsymbol{M}_y, \boldsymbol{M}_u)$ depends on $\boldsymbol{M}_y$ and $\boldsymbol{M}_u$, which are part of the sought solution. A solution may then consist in choosing them heuristically. However, there is no guarantee of the optimal solution. To solve this problem, a SDP (Semi Definite Programming) formulation is derived in [131, 132] by means on the bounded real lemma [29] and the projection lemma [100].

Since the conditions stated by (1.122) and (1.124) are only sufficient conditions, what is the degree of conservatism of the obtained solution $(\boldsymbol{M}_y, \boldsymbol{M}_u, \boldsymbol{L}(s))$? The FDI filter design method described in the previous section does not account for the structure of the model perturbation block Δ. This means that the solution $(\boldsymbol{M}_y, \boldsymbol{M}_u, \boldsymbol{L}(s))$ can be conservative in some cases. Furthermore, the condition $\gamma > 1$ does not imply with certainty that the FDI filter does not meet the desired H_∞/H_- specifications.

To check if the required performances are achieved, the robust test based on the generalized structured singular value (denoted μ_g) proposed in [131, 133, 134] can be used. Robust stability, i.e., stability of all models in the model set $(\Delta(s) * \boldsymbol{P})$, is analyzed with the μ-function. The real-valued function μ is the inverse of the size of the smallest destabilizing perturbation Δ [67]. Consequently, μ-analysis guarantees stability for perturbations up to $1/\mu$. In a μ_g-problem, the perturbation structure Δ is divided into two parts, say Δ_J and Δ_K, so that Δ_J satisfies a maximum norm constraint and Δ_K a minimum gain constraint [134]. The analogous stability result is that the system is stable for $\|\Delta_J\|_\infty < 1/\mu_g$ and for $\|\Delta_K\|_\infty > \mu_g$.

To formalize, consider a block structure $\underline{\Delta} = \{\mathrm{diag}(\Delta_J, \Delta_K)\}$ and a complex valued matrix

$$\boldsymbol{N} = \begin{pmatrix} \boldsymbol{N}_{JJ} & \boldsymbol{N}_{JK} \\ \boldsymbol{N}_{KJ} & \boldsymbol{N}_{KK} \end{pmatrix} \tag{1.125}$$

partitioned in accordance with $\underline{\Delta} = \{\mathrm{diag}(\Delta_J, \Delta_K)\}$ that satisfies the closed-loop equations

$$\boldsymbol{z} = \boldsymbol{N}\boldsymbol{v}, \quad \boldsymbol{v} = \Delta\boldsymbol{z}, \quad \boldsymbol{z} = \begin{pmatrix} \boldsymbol{z}_J \\ \boldsymbol{z}_K \end{pmatrix}, \quad \boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_J \\ \boldsymbol{v}_K \end{pmatrix} \tag{1.126}$$

The μ_g-function is a positive real-valued function of the matrix $\boldsymbol{N}$ and the specified block structure $\underline{\Delta}$ defined according to

$$\mu_{g\underline{\Delta}}(\boldsymbol{N}) = \max_{\|v\|=1} \left\{ \gamma : \begin{array}{ll} \|v_j\|\gamma \leq \|z_j\|, & \forall j \in J \\ \|v_k\| \geq \|z_j\|\gamma, & \forall k \in K \end{array} \right\} \tag{1.127}$$

The μ_g function is defined in a domain $\mathrm{dom}(\mu_g)$ given by

$$\boldsymbol{N} \in \mathrm{dom}(\mu_g) \quad \text{iff} \quad \boldsymbol{N}_{KK}\boldsymbol{v}_K = 0 \Rightarrow \boldsymbol{v}_K = 0 \tag{1.128}$$

which is equivalent to a nontrivial solution, i.e., the maximisation part in the μ_g problem is finite.

To solve the robust fault sensitivity performance analysis problem with no conservativeness, consider the block diagram depicted in Fig. 1.8 and the shaping filters $\boldsymbol{W}_d$ and $\boldsymbol{W}_f$ given by (1.120). Including $\boldsymbol{K}$, $\boldsymbol{M}_y$, $\boldsymbol{M}_u$, $\boldsymbol{L}$ and the shaping filters $\boldsymbol{W}_d$ and $\boldsymbol{W}_f$ into the model $\boldsymbol{P}$ leads to the set up described by the block diagram shown in Fig. 1.10. Disturbance signal$\tilde{\boldsymbol{d}}$ is defined

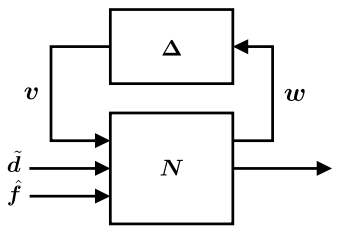


Figure 1.10 – The generic structure of robust detection performance analysis problem

as in Fig. 1.9 and $\tilde{\boldsymbol{f}}$ is a fictitious signal defined according to

$$\tilde{\boldsymbol{f}}(s) = \boldsymbol{W}_f(s)\boldsymbol{f}(s) \tag{1.129}$$

The filter performances analysis problem over the plant perturbations $\Lambda \in \underline{\Lambda}$ is then a min-max gain problem over the specified frequency grid Ω. This problem can be formulated as

$$\sup_{\omega\in\Omega} \overline{\sigma}\left(\boldsymbol{T}_{r\tilde{d}}(j\omega)\right) < 1, \quad \forall\Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.130}$$

$$\inf_{\omega\in\Omega} \underline{\sigma}\left(\boldsymbol{T}_{r\tilde{f}}(j\omega)\right) > 1, \quad \forall\Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1 \tag{1.131}$$

where $\boldsymbol{T}_{r\tilde{d}}$ and $\boldsymbol{T}_{r\tilde{f}}$ denote respectively the closed loop transfer between $\boldsymbol{r}$ and $\tilde{\boldsymbol{r}}$, and between $\boldsymbol{r}$ and $\tilde{\boldsymbol{f}}$. The following theorem gives the solution of the robust fault sensitivity analysis problem.

Theorem 1.4 (Henry and Zolghadri [132])**.** *Consider the model structure depicted in Fig. 1.10 and partition $\boldsymbol{N}$ according to $\boldsymbol{N} = \begin{pmatrix} \boldsymbol{N}_{11} & \boldsymbol{N}_{12} \\ \boldsymbol{N}_{21} & \boldsymbol{N}_{22} \end{pmatrix}$, where $\boldsymbol{N}_{22}$ denotes the transfer between the signals $\boldsymbol{r}$ and $\tilde{\boldsymbol{f}}$. Let $\sup_\omega \mu_{\overline{\underline{\Delta}}}(\boldsymbol{N}_{11}(j\omega)) < 1$ where $\overline{\underline{\Delta}} = \{diag(\Delta, \Delta_d)\}$ where $\Delta_d \in C^{dim(\tilde{d})\times dim(r)}$ is a fictitious plant perturbation block introduced to closed the loop between $\boldsymbol{r}$ and $\tilde{\boldsymbol{d}}$, and let $\boldsymbol{N} \in dom(\mu_g)$. Then a necessary and sufficient condition for* (1.130)-(1.131) *to hold is*

$$\sup_{\omega\in\Omega} \mu_{g\tilde{\underline{\Delta}}}(\boldsymbol{N}(j\omega)) < 1 \tag{1.132}$$

The block structure $\tilde{\underline{\Delta}}$ is defined according to $\tilde{\underline{\Delta}} = \left\{diag(\bar{\Delta}, \Delta_f)\right\}$, where $\Delta_f \in C^{dim(\tilde{f})\times dim(r)}$ is a fictitious uncertainty block introduced to close the loop between $\boldsymbol{r}$ and $\tilde{\boldsymbol{f}}$.

The requirement $\sup_\omega \mu_{\overline{\underline{\Delta}}}(\boldsymbol{N}_{11}(j\omega)) < 1$ is equivalent to the maximum norm constraint in (1.130)-(1.131) is satisfied over the block structure $\underline{\Delta}$, which is strictly equivalent to the robustness performance specification (S.1), i.e., $\forall\Delta \in \underline{\Delta} : \|\Delta\|_\infty \leq 1$.

Because this theorem involves a necessary and sufficient condition which takes into account the structure of the model perturbations Δ, the robust sensitivity performance (i.e., the specification (S.2)) can be tested by calculating the μ_g function of $\boldsymbol{N}$ over the block structure $\tilde{\underline{\Delta}}$. Computationally inexpensive upper and lower bounds have been developed in [199]. If the bounds are equal, then an exact value of μ_g has been found. An upper bound of μ_g can be formulated as a convex optimization problem, which results in checking a LMI feasibility [128]. A lower bound algorithm from the "Power Algorithm" family is also proposed in [199], which seeks to optimize Δ_J and Δ_K explicitly.

Remark 1.17. *An important point regarding the robust fault sensitivity test given by* (1.132) *is that the convergence of the upper bound is much more critical than the lower, as the problem is to check if* μ_g *(or any upper bound) is below* 1 *or not.*

Remark 1.18. *The* H_∞/H_- *technique has been extended within the LPV setting in a numerous recent papers. These techniques consider both the so-called polytopic [113, 130, 137] and the LFR [129, 130, 137] formalism.*

- **Application to Space Systems**
  - **Satellite Microscope**

Microscope is a satellite that has the mission of testing the equivalence principle, which postulates the equality between gravitational mass and inertial mass with a resolution almost 3 orders of magnitude more than the best tests so far performed on Earth, see Fig. 1.11 for an illustration performed by the CNES-France. To control its trajectory, Microscope uses the coupling of six ultra-sensitive accelerometers, a stellar sensor and a very precise electric propulsion system composed by 12 Field Emission Electric Propulsion (FEEP) thrusters. The mission can be in danger if a FEEP thrusters fault occurs, since the satellite may not compensate for non-gravitational disturbances (i.e., atmospheric drag and solar radiation) which are indispensable prior conditions for its mission: testing the Equivalence Principle.

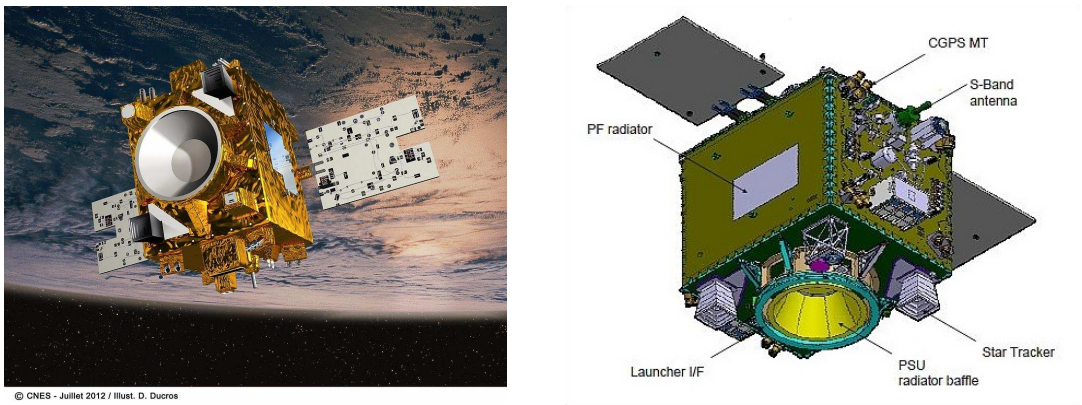


Figure 1.11 – The Microscope satellite, ©2006/2012 CNES

A solution to this problem was proposed in [126], where a bank of 12 H_∞/H_- residual generators was used for FDI purposes. To be more precise, the design was done so that the sensitivity level of the ith residual with respect to the ith FEEP thruster fault f_i is maximised in the H_- norm sense, whilst guaranteeing robustness against measurement noises and spatial disturbances in the H_∞ norm sense. Nonlinear simulations show that, despite the fact that the considered faults are fully compensated by the control law, the faults are successfully detected and isolated.

  - **The HL-20 RLV**

A HL-20 reusable launch vehicle (RLV) is a launch system which is capable of launching a launch vehicle into space more than once (for more information see the application paragraph of Section 1.3.3.1). A typical atmospheric re-entry for a medium or high Lift/Drag (L/D) vehicle consists of performing three successive flight phases. During the last phase

of the atmospheric reentry mission (the landing phase), control is achieved using only aerosurfaces, and the occurrence of faults is a critical issue as they could lead quickly to vehicle-control loss. The time delay to engage recovery actions is therefore very limited, and so, a reliable and robust FDI unit appears to be a key feature in the overall system-health monitoring.

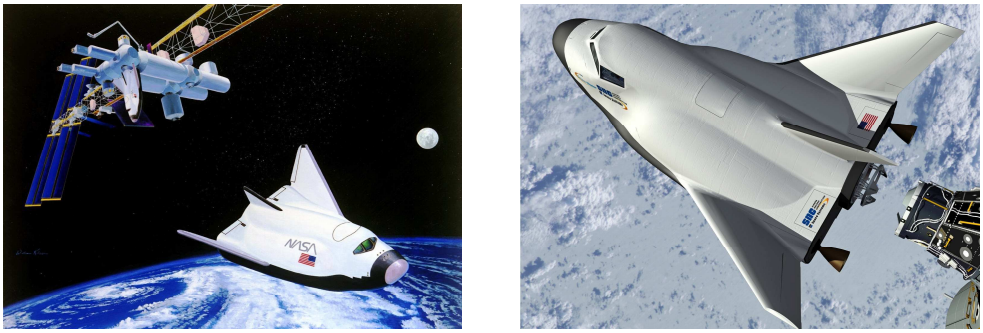


Figure 1.12 – Artist's concept of an HL-20 at a space station, ©1992 NASA

The work presented in [88] deals with any type of faults in the wing flap actuators during the landing phase. The strategy proposed by the authors consists of a bank of two H_∞/H_- fault detection filters that are designed so that a given filter is made robust against measurement noise, guidance reference signals, winds turbulence, and faults in a given wing flap actuator, whilst remaining sensitive to all faults in the other wing flap actuator. For the purpose of estimating the position of the faulty control surfaces, the nonlinear EKF method presented in [85, 86] is used.

– **LISA Pathfinder**

The LISA Pathfinder (LPF) will pave the way for a major ESA/NASA mission planned for the near future: LISA (Laser Interferometer Space Antenna), aimed at detecting low-frequency gravitational waves of very massive cosmic objects (e.g., black holes) from space. The primary scientific objectives of the LPF experiment mainly consists in placing two test masses in a nearly perfect gravitational free-fall, and of controlling and measuring their motion with unprecedented accuracy of about 3×10^{-14} m/s$^2/\sqrt{\text{Hz}}$ in a measurement bandwidth between 1 mHz and 30 mHz.

Among key technologies to be tested, attractive and important features rely on high accuracy electrostatic-based inertial sensors, high resolution laser interferometer, star trackers. The electrostatic actuation system consists of a set of 12 FEEP thrusters and of a set of 8 micro-Newton colloidal thrusters in charge of controlling the spacecraft and the test masses during the experiment phase. The Fig. 1.13 illustrates the LPF spacecraft and a internal view of the LISA technology package consisting of the two test masses, the optical bench, and the metrology systems.

The colloidal thrust system is a real cornerstone for the success of the experiment and the occurrence of faults could lead to significant experiment objectives degradation or mission unavailability according to the in-placed controllers fault accommodation capabilities. Falcoz et al. [87] considered the problem of faults affecting the micro-Newton colloidal thrust system of the LPF experiment. The first FDI scheme consists of a bank of eight Kalman-

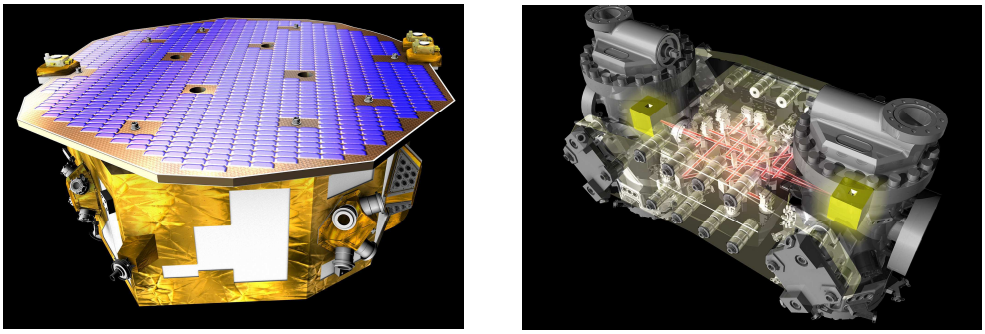


Figure 1.13 – LISA Pathfinder and its technology package, ©2011 ESA

based observers and the second strategy is based on a bank of eight H_∞/H_- filters to generate residuals robust against spatial disturbances (i.e., third-body disturbances, J2 disturbances, atmospheric drag and solar radiation pressure), measurement noises and sensor misalignment phenomena, whilst guaranteeing fault sensitivity performances.

– **Telecom Satellites**

The FDIR strategies used in the telecommunication satellite market requires a strong robustness and minimization of mission outage. One of the most fault sensible subsystem is the Attitude and Orbit Control System (AOCS) that needs to be more deeply investigated. The telecommunication satellite consists of a set of Gyro (measuring roll and yaw axis angular rates) and IRES (roll and pitch attitude angles) sensors. A typical telecom satellite is also equipped with 3 reaction wheels and two chains of 7 thrusters (10N) to control the position. The industrial reconfiguration logic rest in cold redundancy, i.e., the faulty thruster chain is passivated and switched on the redundant thruster chain. The development of robust and reliable model-based FDI rest in quick thruster fault detection during the *station keeping manoeuver* to limit the mission outage, as well as in improvement of the fault coverage in order to optimize spacecraft life cycle and telemetric bandwidth saving. A common FDI techniques for telecom satellites are based on a bank of H_∞/H_-, pure H_∞ or Kalman filters, respectively.

– **The MSR Rendezvous Mission**

The work reported in [136] addresses the design of model-based FDI schemes to detect and isolate faults occurring in the orbiter thruster unit during the rendezvous phase of the Mars Sample Return (MSR) mission. The proposed fault diagnosis method is based on a $H(0)$ filter with robust poles assignment to detect quickly thruster faults and a cross-correlation test between the residuals and the thrusters signals to isolate them. Simulation results from the high-fidelity nonlinear simulator demonstrate that the proposed method is able to diagnose thruster faults with a detection and isolation delay less than 1.1 s for a certain type of faults (single thruster opening at 100%).

1.3.5 Decision Test

The first step of a fault diagnosis procedure is to evaluate the residuals. A fault can be detected by comparing the residual evaluation function $J_{ev}(\boldsymbol{r}(t))$ with a threshold function $J_{th}(t)$

according to the following hypothesis test:

$$\begin{aligned} H_0: &\quad J_{ev}(\boldsymbol{r}(t)) \leq J_{th}(t) \qquad \text{if fault-free} \\ H_1: &\quad J_{ev}(\boldsymbol{r}(t)) > J_{th}(t) \qquad \text{if faulty} \end{aligned} \tag{1.133}$$

where H_0 corresponds to the zero hypothesis meaning normal operation ($\boldsymbol{f}(t) = \mathbf{0}$) and H_1 to the hypothesis that the system is in abnormal operation mode ($\boldsymbol{f}(t) \neq \mathbf{0}$).

There are many ways of defining $J_{ev}(\boldsymbol{r}(t))$ and $J_{th}(t)$. The simplest approach is to decide that a fault has occurred when the instantaneous value of a residual evaluation function $J_{ev}(\boldsymbol{r}(t))$ exceeds a constant threshold J_{th}.

When a *constant threshold* is used, the sensitivity to faults will be intolerably reduced if the threshold is chosen too high, whereas the false alarm rate will be too large when the threshold is chosen too low. The proper choice of the threshold is a delicate problem [223].

One of the approach to overcome the above proposed difficulty is to use a time varying threshold function $J_{th}(t)$. This approach is also called the *adaptive threshold* approach and can be found in many publications [81, 95, 141]. This concept is illustrated in Fig. 1.14 which also shows the typical shape of an adaptive threshold for direct residual evaluation.

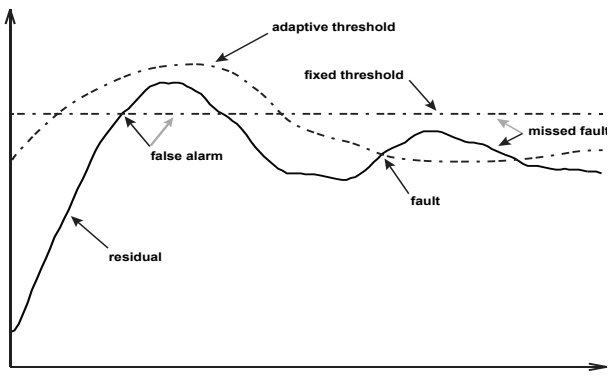


Figure 1.14 – Adaptive threshold

Due to uncertainty, disturbance and noise encountered in a practical application, one will rarely find a situation where the conditions for a perfectly robust residual generation are met. It is practically impossible to detect a fault with unlimited sensitivity. Obviously, finding a compromise between the sensitivity and disturbance attenuation of the methods is an important design issue. It is therefore necessary to provide sufficient robustness not only in the residual generation stage, but also at the decision-making stage [223].

In some applications, stochastic system models are considered and the residuals generated are known or assumed to be described by some probability distributions [143]. Most statistical tests assume a normal distribution for $\boldsymbol{r}$ and require the knowledge of its nominal mean μ_0 and variance σ_0^2. Robust decision making tools use the history and trend of the residual and make use of powerful or optimal statistical test techniques. The well-known examples of these statistical test techniques are the following[7].

- **Statistical thresholding (3-sigma rule) test:** The idea behind this test is to choose the two-sided threshold according to: $J_{th} = \mu_0 \pm k\sigma_0$, where $k \geq 3$ [247]. This approach

[7]To present the main statistical tests, a scalar residual r is considered.

relies on the fact that 99.7% of the points of a Gaussian distribution lie within 3σ of its mean. Thus, this simple test is able to detect large deviations in $\boldsymbol{r}$, but is likely to miss a detection when the size of the change is within the same order of magnitude as the $3\sigma_0$ of the process. When bounds on model uncertainties, disturbances and noise are available, then the approach given in [81] provides a robust version of statistical thresholding in the worst-case sense (thus conservative). A similar problem is addressed in [63], where the threshold calculation is based on LMI-technique.

- **Generalized Likelihood Ratio (GLR) test:** The evaluation function $J_{ev}(\boldsymbol{r}(t))$ of this test is based on the likelihood ratio of the probability that the mean of $\boldsymbol{r}$ is $\mu_1 \neq \mu_0$ to the probability that it is μ_0, where μ_1 is the mean of $\boldsymbol{r}$ in faulty situation [10, 60]. This test still assumes that, both μ_0 and σ_0^2, are known a priori. See a more detailed discussion about this test in the Appendix B.

- **Sequential Probability Ration Test (SPRT):** Similarly to the GLR test, this test utilizes the likelihood ratio. The advantage of this method is that the threshold is fully determined by fixing the desired false alarm and desired the non-detection rate [10, 287]. Compared to GLR, this test introduces a *no decision* stage, when more data are collected in order to decide between H_0 and H_1. In the frame of fault diagnosis, this can be interpreted as a non-faulty behaviour, i.e., H_0. This test is also known as Wald's sequential test, see Appendix B for further discussion about this test.

- **CUSUM test:** This test was announced few years after the publication of Wald's SPRT algorithm by Page [220]. Only few statistical hypotheses are needed for this two-sided test, which is expressed as follows [10, 19]

$$\begin{aligned} S^+(t) &= \max\left(S^+(t-1) + r(t) - \mu_0 - \delta_{\mu_0}/2, 0\right) \\ S^-(t) &= \max\left(S^-(t-1) - r(t) - \mu_0 - \delta_{\mu_0}/2, 0\right) \end{aligned} \tag{1.134}$$

  where δ_{μ_0} is assumed to be know and represents the shift in the mean value after the fault, i.e., either an increase $\mu_1^+ = \mu_0 + \delta_{\mu_0}$ or a decrease $\mu_1^- = \mu_0 - \delta_{\mu_0}$ in the mean. Then, the H_1 hypothesis is accepted at the alarm time

$$t_a = \min\{t : (S^+(t) \geq J_{th}) \cup (S^-(t) \geq J_{th}\} \tag{1.135}$$

  where J_{th} is again some tunable threshold reflecting the desired false-alarm rate.

- **Student's t-test:** This test the null hypothesis H_0, i.e., checks whether the residual follows a normal distribution $r \sim \mathcal{N}(\mu_0, \sigma_0^2)$. This leads to an automatic thresholding given by Student's table with a required confidence level (e.g., 95%) [112]. If this threshold is crossed, then the H_1 is adopted.

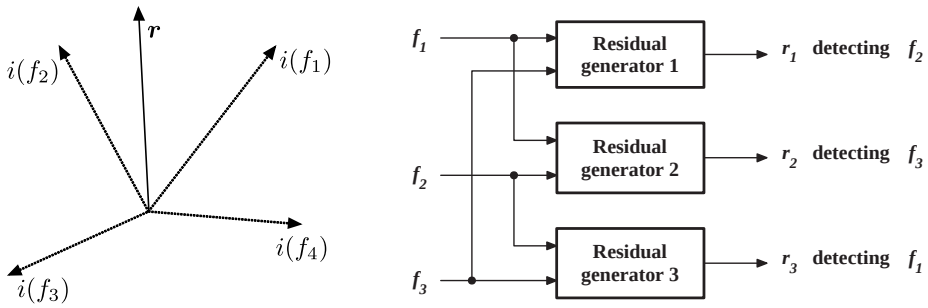
A good survey about other statistical decision making tools can be found in [10, 116, 143].

1.3.6 Fault Isolation

The residuals generated should not only be able to detect the faults, they need to be able to determine the exact location of the fault (which component has failed). The conditions for a

existence of a perfect fault isolation can be found in Ding [60]. In the FDI[8] literature two main approaches for fault isolation exist:

- **Directional residual approach:** The directional residual approach achieves the isolation task by generating residual vectors that lie in a specified direction in the residual subspace corresponding to each type of fault (see Fig. 1.15a for illustration). The fault isolation problem is then transformed into one of determining the direction of the residual vector [39, 282].
- **Structured residual approach:** The structured residual approach is focused on developing a bank of residual generators (see Fig. 1.15b for illustration) to be sensitive to a single or selective set of faults, and insensitive to the rest [48, 93, 106]. Various design



(a) directional residual approach (b) structured residual approach

Figure 1.15 – Fault isolation

schemes exists [93]. A popular approach is the *dedicated observer scheme* proposed by Clark [48] where each observer is driven by a different single sensor output and the complete output vector $\boldsymbol{y}$ is estimated. This scheme is capable to detect and isolate multiple simultaneous faults by checking properly structured sets of observer errors with the aid of a threshold logic [93]. If, for example, a certain sensor fault occurs, then the related output estimate reconstructed by the corresponding observer will be destroyed which can be then identified by an appropriate isolation logic. This philosophy is known as the "column matching" approach [105].

Frank [92] developed an alternative version, i.e. the so-called *generalized observer scheme* that provides an observer dedicated to a certain sensor fault and driven by all outputs except that of the respective sensor. This scheme allows one to detect and isolate only a single fault in any of the sensors, but with increased robustness with respect to the unknown inputs.

The application of the UIO (see Section 1.3.2.2) philosophy to actuator, sensor or component Fault Detection and Isolation can bring a trade-off to the above mentioned two approaches. The general structure of the robust observer scheme based on UIOs is depicted in Fig. 1.16. For the sake of simplicity, assume that m different faults f_i can occur in the system where m is also the number of measurements available. There exists three extremes [93]:

Faults have to be only detected: The FDI scheme reduces to a single UIO that

[8]There exists an other community called DX for Diagnosis, that addresses the problem of fault isolation. Their approaches use AI-based tools to perform the diagnosis task, see e.g., [15, 52, 56, 211, 212, 249]

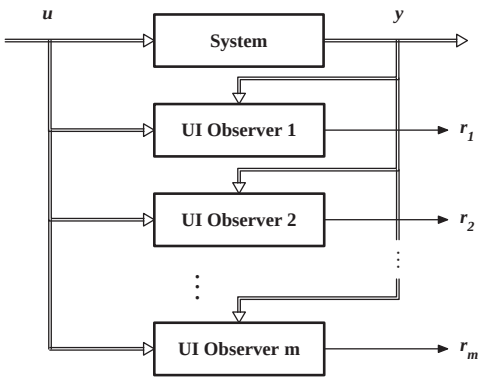


Figure 1.16 – General structure of the UIO scheme

generates a residual that is sensitive to all faults whilst being robust to $m-1$ unknown inputs. This design freedom can be used to generate a residual that is robust to the maximum number of unknown inputs, but not providing isolation properties.

Only a single fault is to be detected and isolated: Here the FDI scheme allows fault isolation and let the maximum design freedom for the generation of robustness to unknown inputs. Thus, the ith observer ($i = 1, 2, \ldots, m$) is designed to be insensitive to the ith fault f_i and to $m-2$ unknown inputs. Here the f_i is interpreted as an unknown input and the remaining design freedom is used for generating invariance to the unknown inputs. Repeating this design m times one arrives at an UIO scheme according to Fig. 1.16. Here the first residual r_1 depends on all faults except of the first f_1, the second residual r_2 on all except the second fault f_2 and so on. Mathematically speaking

$$\begin{cases} r_1 = q_1(f_2, f_3, \ldots, f_m) \\ \quad\vdots \\ r_i = q_i(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m) \\ \quad\vdots \\ r_m = q_m(f_1, \ldots, f_{m-1}) \end{cases}$$

Hence a simple decision logic can be implemented [93]. Note, that only a single fault at a time can be detected.

All faults are to be detected and isolated: To be able to detect and isolate all faults occurring simultaneously, one has to implement all faults, except the ith fault, in the ith UIO as unknown inputs. Therefore the rank of the unknown input distribution matrix $\boldsymbol{E}$ is increased by $m-1$, which is the largest possible rank of $\boldsymbol{E}$ for which complete invariance can be achieved. In this case, the observer cannot be made robust with respect to any unknown input. The residuals depend on the faults according to the following relations

$$\begin{cases} r_1 = q_1(f_1) \\ r_2 = q_2(f_2) \\ \quad\vdots \\ r_m = q_m(f_m) \end{cases}$$

This allows to uniquely detect and isolate m faults even if they occur simultaneously. The price to pay is the loss of robustness with respect to unknown inputs [93].

1.3.7 Fault Identification

Fault identification (also called fault estimation) follows after fault isolation and is defined as the procedure of determination of the size (magnitude) and time-variant behaviour (shape) of the faults [147]. The fault identification methods generally obey to the ones presented in Section 1.3.2.4 and Section 1.3.3. Fault identification is needed in certain fault accommodation approaches, i.e., the control law is adapted based on the FDD in order to recover acceptable control of the system subject to faults [19].

Several methods for fault estimation [312] have been developed, such as:

- sliding mode observer [6, 76, 77, 273, 274],
- learning methods based on neural network [165, 243, 244], and
- adaptive observer technique [151, 291, 307, 309].

Nonlinear approaches, especially SMOs, have good robustness and are completely insensitive to matched uncertainty [76, 281]. However, some systems may fail to satisfy the condition of the coordinate transformations [307]. Learning methods based on neural network require that all of the system states are measurable [243]. Adaptive methods for actuator faults were developed in Wang and Daley [291] and Jiang et al. [151].

1.4 Active Fault-tolerant Control Approaches

As an emerging and active area of research in automatic control, fault-tolerant control has recently attracted more and more attention. This section gives a review of different methods of controller re-design approaches and mechanisms achieving fault tolerance, ranging from projection-based methods to control signal redistribution. Since FTCSs involve many disciplines, there are many related publications in each individual topic in AFTCS and it is difficult to include all of them in the state of the art. However, it is believed that the references on articles and books cited in this section would serve the reader as good resources for entry and further study.

An overview and introduction into the field has been proposed by [183, 224]. A recent and very extensive bibliographical review has been published by Zhang and Jiang [312]. Other recent bibliography references can be found in [19, 151, 210, 285, 303]. Historically, FTC solutions have been developed for civil and military aircrafts, and recently UAVs and Re-entry vehicles, see [33, 188] and the book [78] written by the GARTEUR FM-AG16 members.

Despite the fact that some survey papers exist on FTC, the approaches are not very well classified as opposed to the FDI/FDD methods. Thus, the classification illustrated in Fig. 1.17 is proposed in this thesis. This classification is inspired by the work of Lunze and Richter [183] and serves as a guideline for the here considered methods. An approach which is not introduced in the following is based on the primal and dual-Youla parametrization, proposed by Niemann and

Stoustrup [206]. It is to be discussed since it represents some attractive advantages for FTC.

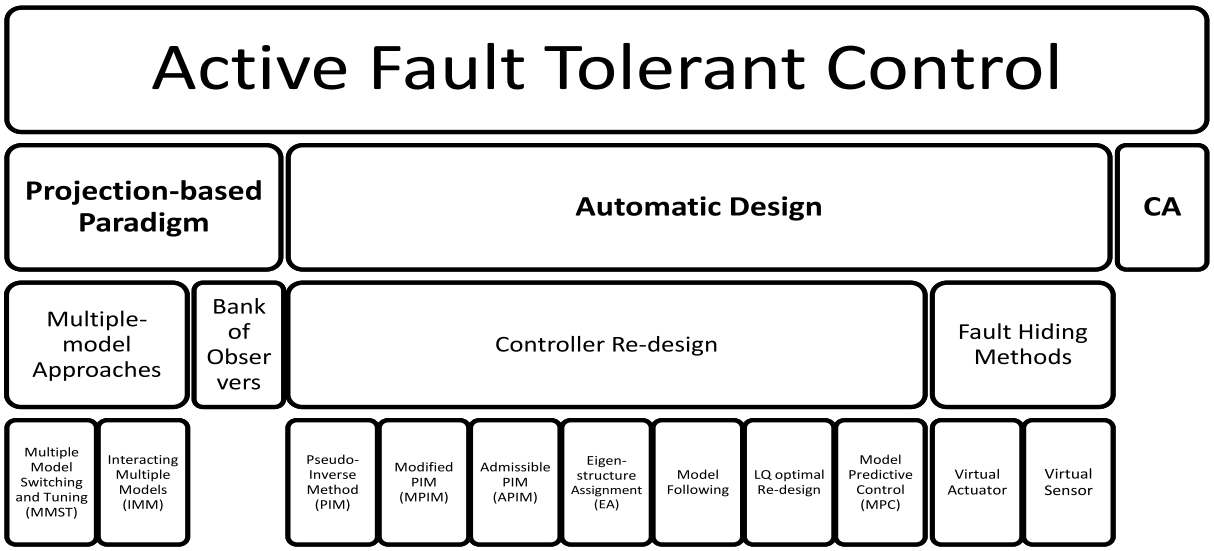


Figure 1.17 – Control re-design approaches

1.4.1 Projection-based Paradigm

1.4.1.1 Multiple-Model Approach

The multiple-model (MM) approach belongs to the so called *projection-based* techniques [192, 203, 277]. This approach is used for systems, where the nominal (robust) controller cannot provide all the goals (stability and performance) in the presence of faults. The main idea is based on the existence of a suitable set of pre-computed controllers for each fault mode, as shown in the Fig. 1.18. In this sense, this approach can be classified into the class of pre-computed FTC solutions.

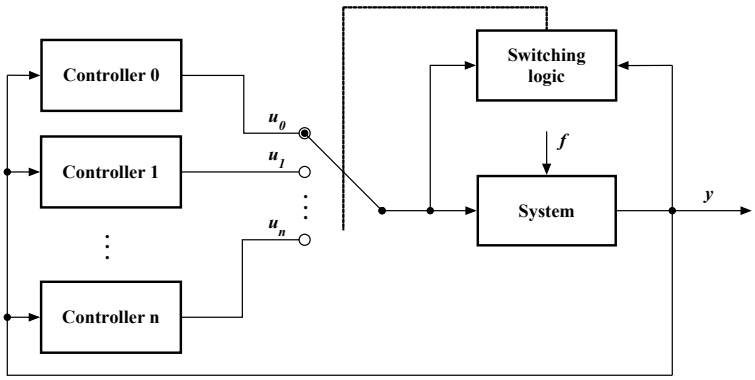


Figure 1.18 – Structured scheme of the multiple-model approach

In the MM approach, a bank of parallel models is used to describe the system under normal conditions and under a finite set of failure modes, such as actuator or component faults. A reasonable controller is designed for each of these models. A suitable chosen switching logic is

used to determine the mode of the system at each time step, and to select the corresponding controller that has been designed for that particular mode. This results in robust and improved performance under various operating conditions. Note that this scheme can principally only cover a set of anticipated faults. This approach, however, assumes that for each fault an appropriate controller has been designed before the plant is put into operation. From a practical aspect, this is not reasonable if a large number of faults has to be considered.

A solution to this problem may consist in approach proposed by Staroswiecki and Berdjag [266] that proposed to use jointly and adequately passive and active FTC laws. This may allow one to cover a large number of faulty situations.

In the area of AFTC, two main approaches can be distinguished: Multiple Model Switching and Tuning (MMST) and Interacting Multiple Models (IMM). When a fault occurs MMST switches to a pre-computed control law corresponding to the current failure situation. Rather than using the model which is closest to the current fault scenario, IMM computes a fault model as a convex combination of all pre-computed fault models and then uses this new model to make control decisions. These methods are further presented in the following sections.

• Multiple Model Switching and Tuning

In the MMST technique shown in Fig. 1.19, the dynamics of each fault scenario are described by a dedicated model. Each model is paired with its respective controller. The general form of this approach with a linear system is shown in the following equations

$$\mathcal{S} : \begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}_0(\boldsymbol{p}(t))\boldsymbol{x}(t) + \boldsymbol{B}_0(\boldsymbol{p}(t))\boldsymbol{u}(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}_0(\boldsymbol{p}(t))\boldsymbol{x}(t) \end{cases} \tag{1.136}$$

where the vector $\boldsymbol{p}(t) \in \mathcal{S} \subseteq \mathbb{R}^l$ represents the unknown plant parameters which may vary in time in an abrupt fashion and represents the various failure scenarios.

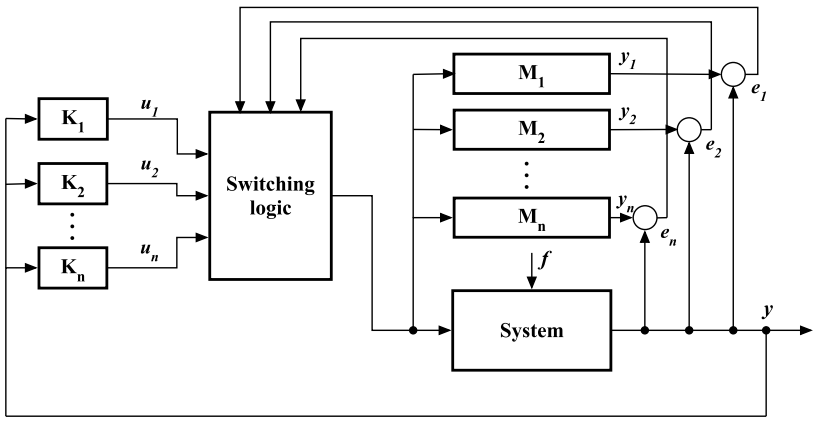


Figure 1.19 – Multiple model switching and tuning scheme

Let $\mathcal{M}$ be the finite set of n linear models

$$\mathcal{M} : \{M_1, \ldots, M_n\} \tag{1.137}$$

such that

$$M_i : \begin{cases} \dot{\boldsymbol{x}}_i(t) = \boldsymbol{A}_i \boldsymbol{x}_i(t) + \boldsymbol{B}_i \boldsymbol{u}(t) \\ \boldsymbol{y}_i(t) = \boldsymbol{C}_i \boldsymbol{x}_i(t) \end{cases} \tag{1.138}$$

where model M_i corresponds to a set of parameters $\boldsymbol{p}_i \in \mathcal{S}$. For each model M_i a stabilizing controller $\boldsymbol{K}_i$ is designed (off-line).

A switching logic module computes for each model M_i a performance index J_i, which is a function of the error $\boldsymbol{e}_i$ between the model M_i and the measurements data at time t. The performance index J_i is of the following form [203]

$$J_i(t) = \alpha e_i^2(t) + \beta \int_0^t e^{-\lambda(t-\tau)} e_i^2(\tau) d\tau, \qquad \alpha \geq 0, \;\; \beta > 0, \;\; \lambda > 0 \tag{1.139}$$

The coefficients α and β are responsible for the tradeoff between instantaneous and long-term contributions of the error e_i in the calculation of the index J_i. The coefficient λ is used as a forgetting factor.

The model M_i producing the smallest performance index J is the closest to the current system, and therefore the controller $\boldsymbol{K}_i$ becomes active.

Most of the MMST reconfigurable schemes also include a tuning part, which is based on a separate identification algorithm that updates the parameters of the model M_i while the controller $\boldsymbol{K}_i$ is active.

The MMST technique has the advantages of being fast and usually stable if the actually occurring fails match the predefined fault scenarios. However, the main limitation is that there may be faulty scenarios that were not modelled, which would likely be the case for multiple or structural faults. Moreover, the number of individual pairs of $M_i/\boldsymbol{K}_i$ to be designed, may become excessively large if the system has to be successfully operate over a wide range of fault scenarios [27, 69].

Remark 1.19. *Note that such a control switching structure is classified by some authors as the supervisory FTC structure [19, 26]. In this case, the main problem is concerned by the global stability of the overall FTC scheme [301, 302] A solution to this problem is given by Efimov et al. [79, 80] using the so-called dwell-time approach. This technique will be discussed in more details in Section 1.4.4.1.*

• Interacting Multiple Models

The IMM approach attempts to deal with the main limitation of the MMST technique, i.e., that every fault scenario must belong to the model set $\mathcal{M}$.

The primary assumption of IMM is that every possible fault can be modelled as a convex combination of models [306] in a pre-determined model set $\mathcal{M}$ as defined in (1.138). The faulty system can be expressed as

$$M_f = \sum_{i=1}^{n} \mu_i M_i = \mu^T \begin{bmatrix} M_1 \\ \vdots \\ M_n \end{bmatrix}, \quad M_i \in \mathcal{M}, \quad \mu_i > 0 \in \mathbb{R}, \quad \sum_{i=1}^{n} \mu_i = 1 \tag{1.140}$$

Fault detection and modelling is then done online by identifying the variables μ_i in (1.140).

Several methods for computing the coefficients μ were proposed in the literature. One is known as Multiple Model Adaptive Estimation (MMAE) method (see e.g., [69, 191]). Here, a bank of Kalman Filters is designed for each $M_i \in \mathcal{M}$, running in parallel. A hypothesis testing algorithm uses the residuals from each Kalman Filter to assign a conditional probability to each fault hypothesis.

Once a fault model has been identified, there are a variety of methods for control law calculation. Ones can use Model Predictive Control (MPC) [159, 161, 184, 185] scheme or EA, see [164, 279, 290, 306] for details. One application of IMM approach has been used to design an integrated fault detection and fault tolerant aircraft flight control [310].

1.4.1.2 Bank of Observers for Sensor Faults

If only sensor faults are considered, it seems intuitive to replace the missing signal by an observed value, since, according to the linear system theory, this should not affect the stability of the control loop. The *generalized observer scheme* (see Section 1.3.6) provides the framework for this approach: a bank of $\dim(\boldsymbol{y})$ output observers is used, where every observer relies on a different set of measurements [92, 93, 144]. Once a sensor fault is detected, an observer is activated which does not depend on this sensor, and the output of this observer is used to replace the faulty sensor, see Fig. 1.20.

This setup solves the diagnosis and reconfiguration problems in an integrated manner, which is advantageous. However, this approach is limited to sensor faults. Clearly, the measurements will be of better quality than the observed values, since disturbances act on the observers. For this reason, the nominal controller should use the measurements. Note that it is predominant to make the best-possible use of certain knowledge, such as using reduced observers whenever possible [183].

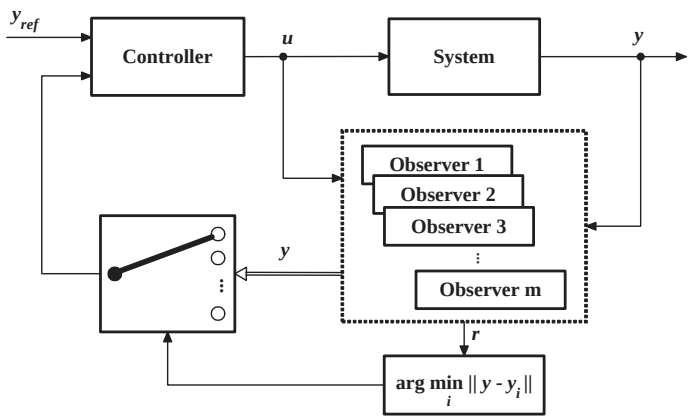


Figure 1.20 – Bank of observers for sensor faults

1.4.2 Automatic Design

1.4.2.1 On-line Controller Re-design

This paradigm covers approaches that perform a complete controller re-design after the detection and identification of a fault. It is clear that in case of a complete component fault, the control structure must change. Both analytical and physical redundancy can be utilized through this paradigm. The computational cost varies according to the specific method.

Several controller re-design methods are available in the literature [183]. Few of them are presented in the following sections: The Pseudo-inverse Method (PIM) with two extensions (modified and admissible), the eigenstructure assignment, the perfect and adaptive model following, the optimal controller design using Linear Quadratic (LQ) optimal control techniques, and the model predictive control. Notably, the model predictive control is not limited to linear systems, whereas most other approaches to date are.

• Pseudo-inverse Method

The PIM addresses actuator and component faults. It is set in a linear control framework with state-feedback control. The basic idea is to match the closed-loop system matrix of the faulty system to the matrix of the nominal system without introducing new states.

Let the nominal system be given by

$$M_0: \quad \dot{\boldsymbol{x}}(t) = \boldsymbol{A}_0\boldsymbol{x}(t) + \boldsymbol{B}_0\boldsymbol{u}_0(t) \tag{1.141}$$

Assume that the nominal closed-loop system is designed by using the linear state feedback of the form

$$\boldsymbol{u}_0(t) = -\boldsymbol{K}_0\boldsymbol{x}(t) \tag{1.142}$$

where $\boldsymbol{K}_0 \in \mathbb{R}^{r\times n}$ is the static feedback gain matrix. The closed-loop system is

$$\hat{M}_0: \quad \dot{\boldsymbol{x}}(t) = (\boldsymbol{A}_0 - \boldsymbol{B}_0\boldsymbol{K}_0)\boldsymbol{x}(t) \tag{1.143}$$

which is stable and provides the nominal dynamic performance.

Suppose that the model of the system, in which faults have occurred, is described by the pair $(\boldsymbol{A}_f, \boldsymbol{B}_f)$ provided by an on-line FDI/FDD module, that is, after the fault estimation time t_f, the post-fault system operation and the model is given by

$$\hat{M}_f: \quad \dot{\boldsymbol{x}}(t) = \boldsymbol{A}_f\boldsymbol{x}(t) + \boldsymbol{B}_f\boldsymbol{u}_f(t) \tag{1.144}$$

In post-fault operation, the aim is to design a new control law

$$\boldsymbol{u}_f(t) = -\boldsymbol{K}_f\boldsymbol{x}(t) \tag{1.145}$$

where $\boldsymbol{K}_f$ is the new state-feedback gain to be determined. In the PIM due to Ostroff [218], the objective is to find a $\boldsymbol{K}_f$ such that the resulting closed-loop transition matrix approximates in some sense to the one in (1.143), which represents the reference model $\hat{M}_0$. The resulting new

closed-loop system is

$$\hat{M}_f : \quad \dot{\boldsymbol{x}}(t) = (\boldsymbol{A}_f - \boldsymbol{B}_f \boldsymbol{K}_f)\boldsymbol{x}(t) \tag{1.146}$$

The solution to this problem is obtained by solving the following matrix equation

$$\boldsymbol{A}_f - \boldsymbol{B}_f \boldsymbol{K}_f = \boldsymbol{A}_0 - \boldsymbol{B}_0 \boldsymbol{K}_0 \tag{1.147}$$

whose necessary and sufficient condition for a solution to exist if

$$\mathrm{Im}(\boldsymbol{A}_f - \boldsymbol{A}_0 + \boldsymbol{B}_0 \boldsymbol{K}_0) \subseteq \mathrm{Im}(\boldsymbol{B}_f) \tag{1.148}$$

and an approximate solution for $\boldsymbol{K}_f$ is given by [218]

$$\boldsymbol{K}_f = \boldsymbol{B}_f^{\dagger}(\boldsymbol{A}_f - \boldsymbol{A}_0 + \boldsymbol{B}_0 \boldsymbol{K}_0) \tag{1.149}$$

where $\boldsymbol{B}_f^{\dagger}$ denotes the pseudoinverse of $\boldsymbol{B}_f$, see Appendix A.3.1.

The solution for $\boldsymbol{K}_f$ is then plugged into the loop instead of nominal controller, see Fig. 1.21. For many anticipated faults the feedback gain $\boldsymbol{K}_f$ can be computed off-line and be stored in the control computer. Once the fault has been detected, isolated and identified, the feedback gain is modified. This PIM method has also been used for on-line accommodation for unanticipated faults [32, 218] although it appeared in different forms.

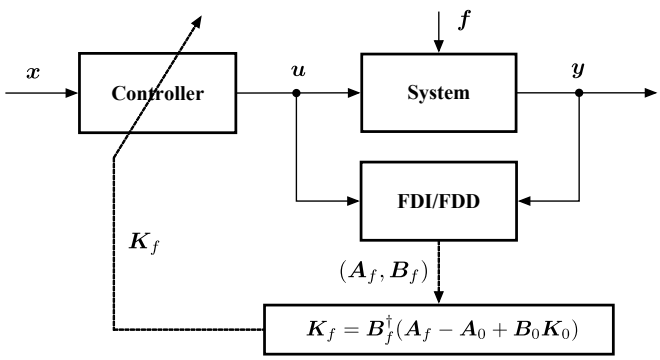


Figure 1.21 – Pseudo-inverse method

Regarding solution (1.149), condition (1.148) will obviously hold only for very particular faults and therefore no exact solution will exist in most fault cases. For this reason, approximate rather than exact solutions might be of interest, i.e., when exact model matching is not possible, an approximate control solution [101] may be computed as

$$\boldsymbol{K}_f^{\sharp} = \arg\min_{\boldsymbol{K}_f} J(\boldsymbol{K}_f) \tag{1.150}$$

by minimizing the criterion

$$J(\boldsymbol{K}_f) = \|(\boldsymbol{A}_0 - \boldsymbol{B}_0 \boldsymbol{K}_0) - (\boldsymbol{A}_f - \boldsymbol{B}_f \boldsymbol{K}_f)\|_F \tag{1.151}$$

where $\|\cdot\|_F$ stands for the Frobenius matrix norm.

However, the distance in the state space between the closed-loop system matrices has no known direct relation to the stability of the system. There is however a connection based on Gershgorin's

theorem on eigenvalue localization [183]. Loosely speaking, if the nominal control loop is robust enough and the norm (1.151) is sufficiently small, then PIM will find a stable solution where the bound in the variations of the closed-loop eigenvalues duo to faults is minimized [101]. One advantage of the PIM is its simplicity in computing the reconfigured feedback controller gain.

The solutions (1.148) and (1.150) are called by some authors as the "Exact Model Matching" and "Approach Model Matching" solutions respectively, see [32, 218, 248, 265, 269].

- **Modified Pseudo-Inverse Method**

A major drawback of the PIM method is that the stability of the reconfigured system cannot be guaranteed. The method has been modified by Gao and Antsaklis [101] in the manner of restrictions on the computation of $\boldsymbol{K}_f$ to guarantee the stability of the post-fault system while achieving as much of the closed-loop nominal performance as possible.

The modification is based upon a consideration of structured uncertainty in the state-space model, i.e., by considering the state-space model with perturbation a matrix $\Delta\boldsymbol{A}_0$, such that

$$\dot{\boldsymbol{x}}(t) = (\boldsymbol{A}_0 + \Delta\boldsymbol{A}_0)\boldsymbol{x}(t) + \boldsymbol{B}_0\boldsymbol{u}_0(t) \tag{1.152}$$

Let assumed that $(\boldsymbol{A}_f, \boldsymbol{B}_f)$, given in (1.144), is a stabilizable pair. It is assumed that a stability bound δ_f can be found such that if

$$|\hat{\boldsymbol{k}}_{f_{i,j}}| < \delta_f, \quad i = 1, 2, \ldots, r \text{ and } j = 1, 2, \ldots, n \tag{1.153}$$

then the system in (1.146) will be stable. Gao and Antsaklis [101] describe in more detail how the bound δ_f can be derived using the method of Zhou and Khargonekar [316] or the method developed by Yedavalli [304].

The algorithm for the Modified Pseudo-inverse Method (MPIM) then becomes as follows:

- **Step 1:** Calculate $\boldsymbol{K}_f$ from (1.149)
- **Step 2:** Check the stability of the closed-loop (1.146) for $\boldsymbol{K}_f$
- **Step 3:** If (1.146) is stable, stop; otherwise calculate $\boldsymbol{K}_f$ using:

$$\boldsymbol{k}_{f_{i,j}} = \begin{cases} \hat{\boldsymbol{k}}_{f_{i,j}} & \text{if } |\hat{\boldsymbol{k}}_{f_{i,j}}| \leq \delta_f \\ \text{sgn}(\hat{\boldsymbol{k}}_{f_{i,j}})\delta_f & \text{otherwise} \end{cases} \tag{1.154}$$

The Fig. 1.21 can also serve as an illustration for this method, since the structure is the same as for PIM. The only difference lies in the details of the design procedure. MPIM solves the stability issue, but it is computationally too intensive to be considered for on-line application [183].

- **Admissible Pseudo-Inverse Method**

As mentioned above, the main shortage of the PIM method is the lack of stability guarantees. The MPIM basically solves the problem under the additional constraint that the resulting closed-

loop system remains stable. This, however, results in a constrained optimization problem that increases the computational burden.

In [265] the classical PIM and the modified PIM have been extended, by using a set of admissible models, rather than searching for an optimal one which does not provide any guarantee about the post-fault system behavior. The approach results in the unique and efficiently computable solutions as well as allows one to characterize the set of accommodable faults, and to quantify the robustness of the fault adaptation scheme with respect to unanticipated faults.

- **Eigenstructure Assignment**

To ensure the closed-loop stability in presence of component failure and to maximize the performance recovery, an eigenstructure assignment based algorithm has been developed under the state [153] and output feedback [68] configurations as an alternative to the pseudo-inverse approach. In this approach, the stability is always guaranteed. Eigenvalues and eigenvectors of the post-fault system can be placed such that the optimal performance recovery is obtained.

More specifically, consider the state space representation of the nominal system given in (1.141). If $\lambda(\boldsymbol{A}_0^c) = \{\lambda_i \in \mathbb{C}, i = 1, 2, \ldots, n\}$ are the eigenvalues of the nominal closed-loop system $\boldsymbol{A}_0^c = \boldsymbol{A}_0 - \boldsymbol{B}_0\boldsymbol{K}_0$, and $\boldsymbol{v}_i \in \mathbb{C}^n, i = 1, 2, \ldots, n$ are the corresponding eigenvectors, the EA method computes the state-feedback gain $\boldsymbol{K}_f$ for the faulty model (1.144) as the solution to the following problem:

$$\boldsymbol{K}_f : \begin{cases} (\boldsymbol{A}_f - \boldsymbol{B}_f\boldsymbol{K}_f)\boldsymbol{v}_i^f = \lambda_i \boldsymbol{v}_i^f \\ \boldsymbol{v}_i^f = \arg\min\limits_{\boldsymbol{v}_i^f} \|\boldsymbol{v}_i - \boldsymbol{v}_i^f\|^2, \quad i = 1, 2, \ldots, n \end{cases} \tag{1.155}$$

In other words, the new gain $\boldsymbol{K}_f$ needs to be such that the eigenvalues of the resulting closed-loop system correspond to the eigenvalues of the nominal closed-loop system and, in addition, the eigenvectors of the closed-loop are as close as possible.

In case of stabilizing output-feedback law

$$\boldsymbol{u}_0(t) = \boldsymbol{K}_0^\circ \boldsymbol{C}_0 \boldsymbol{x}(t) \tag{1.156}$$

where $\boldsymbol{K}_0^\circ \in \mathbb{R}^{r\times m}$ is the static output-feedback gain, the goal is to design a stabilizing controller $\boldsymbol{K}_f^\circ$ for the faulty closed-loop system $\boldsymbol{A}_f - \boldsymbol{B}_f\boldsymbol{K}_f^\circ\boldsymbol{C}_f$ such that the new eigenstructure is as close as possible to that of the original closed-loop system $\boldsymbol{A}_0 - \boldsymbol{B}_0\boldsymbol{K}_0^\circ\boldsymbol{C}_0$. Generally the most dominant eigenvalues of the faulty system, $\{\lambda_i^f, i = 1, \ldots, \max(r, m)\}$ are made to exactly match those of the nominal system λ, while the remainder are kept stable. Similarly, the most important eigenvectors $\boldsymbol{v}_i^f, i = 1, \ldots, \max(m, k)$ of the faulty system are made close to those of the original system $\boldsymbol{v}_i, i = 1, \ldots, \max(m, k)$ in the least squares sense.

There are several limitations to this approach when applied to reconfiguration. Firstly, only linear systems have been considered and actuator limitations have not been taken into account. Secondly, the fault model and FDD uncertainties cannot be easily incorporated in the optimization problem and the effects of possible uncertainties have not been extensively studied. Finally, the effect of the eigenvectors in the faulty system not being exactly equal to those in the nominal system is not well understood. The reference [164] further describes the use of EA.

- **Model-following Approaches**

The basic idea of the linear model-following [280] is an attractive candidate for the re-design process associated with FTC because the goal is to emulate the performance characteristics of a reference model as closely as possible, even in the presence of faults, see [102].

There are basically two strategies:

- **Implicit Model Following (IMF):** The attempt is to change and to adapt the output dynamics of the system using a feedback action in order to equal the output dynamics of a desirable reference model.
- **Explicit Model Following (EMF):** The controller design is based on a real model, which means that the reference model is implemented as part of the actual controller.

The adaptive model following method [163] is a further extension of the basic idea behind PIM. Instead of the closed loop system matrix alone, a closed loop reference model including the reference signal is attempted to be restored.

Consider the nominal system dynamic (1.141) and the output equation given by

$$\boldsymbol{y}(t) = \boldsymbol{C}_0\boldsymbol{x}(t) \tag{1.157}$$

Assuming that the reference model and the system are of the same dimension, let the reference model be described by the following state-space equations

$$\begin{cases} \dot{\boldsymbol{x}}_M(t) = \boldsymbol{A}_M\boldsymbol{x}_M(t) + \boldsymbol{B}_M ref(t) \\ \boldsymbol{y}_M(t) = \boldsymbol{x}_M(t) \end{cases} \tag{1.158}$$

where ref is a reference trajectory signal. The goal is to compute matrices $\boldsymbol{K}_1$ and $\boldsymbol{K}_2$ such that the feedback interconnection of the open-loop system (1.141), (1.157) and the state-feedback control action

$$\boldsymbol{u}(t) = -\boldsymbol{K}_1\boldsymbol{x}(t) + \boldsymbol{K}_2 ref(t) \tag{1.159}$$

matches the reference model. To this end, reference model and closed-loop system are written in the form

$$\begin{cases} \dot{\boldsymbol{y}}_M(t) = \boldsymbol{A}_M\boldsymbol{x}_M(t) + \boldsymbol{B}_M ref(t) \\ \dot{\boldsymbol{y}}(t) = (\boldsymbol{C}_0\boldsymbol{A}_0 - \boldsymbol{C}_0\boldsymbol{B}_0\boldsymbol{K}_1)\boldsymbol{x}(t) + \boldsymbol{B}_0\boldsymbol{K}_2 ref(t) \end{cases} \tag{1.160}$$

so that perfect model following (PMF) can be achieved by choosing

$$\boldsymbol{K}_1 = (\boldsymbol{C}_0\boldsymbol{B}_0)^{-1}(\boldsymbol{C}_0\boldsymbol{A}_0 - \boldsymbol{A}_M) \tag{1.161}$$

$$\boldsymbol{K}_2 = (\boldsymbol{C}_0\boldsymbol{B}_0)^{-1}\boldsymbol{B}_M \tag{1.162}$$

on the assumption that the system has the same number of inputs and outputs (i.e., $m = r$), and that the inverse of matrix $(\boldsymbol{C}_0\boldsymbol{B}_0)$ exists.

If the exact system matrices $(\boldsymbol{A}_0, \boldsymbol{B}_0)$ in (1.161),(1.162) are not known, they can be substituted by some estimated values $(\hat{\boldsymbol{A}}_0, \hat{\boldsymbol{B}}_0)$, resulting in the *indirect (explicit) method* [22]. In order to avoid the need for estimating the system parameters, the *direct (implicit) method* of the model following can be used, which directly estimates the controller gain matrices $\boldsymbol{K}_1$ and $\boldsymbol{K}_2$ by means of an adaptive scheme. Two approaches to direct model following exist, the output error

method [275] and the input error method [114].

• LQ-optimal Re-design

An intuitive approach to the reconfiguration problem is the use of LQ-optimal control. The basic idea is depicted in Fig. 1.22. Before the system is put into operation, a nominal controller is designed off-line using an LQ-optimal design, where the common cost function

$$J = \int_0^\infty (\boldsymbol{x}^T(t)\boldsymbol{Q}\boldsymbol{x}(t) + \boldsymbol{u}^T(t)\boldsymbol{R}\boldsymbol{u}(t))dt \tag{1.163}$$

is minimized. The weight matrices $\boldsymbol{Q}$ and $\boldsymbol{R}$ penalize the state error and the control energy. These matrices are stored for later online reuse. After a fault is detected and identified by the FDI/FDD module, a new controller is designed by solving the Algebraic Riccati Equation (ARE) again with an updated plant model ($\boldsymbol{A}_f$, $\boldsymbol{B}_f$) that reflects the faults. If the faulty system is still controllable, the design will find a controller that solves the control problem with respect to the original criteria (weights) in the best possible way. The main drawback of this approach is that the discarding of the nominal controller completely and the amount of computing resources necessary for LQ design. There are also numerical issues to be aware of, such as the rank deficiency problem [183].

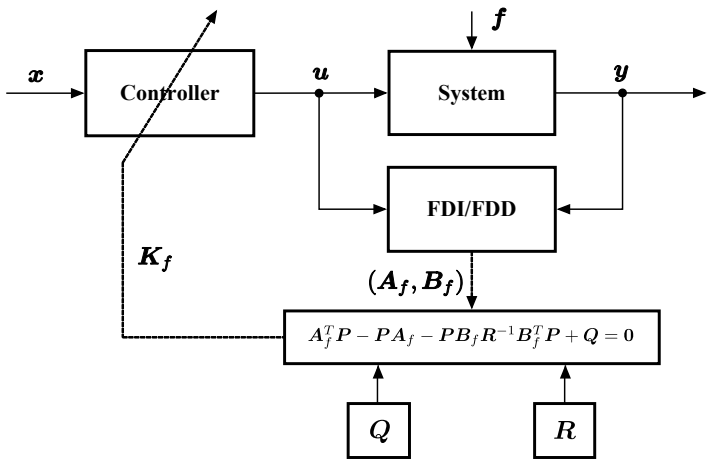


Figure 1.22 – LQ-optimal control re-design

Staroswiecki [264] proposed a progressive accommodation strategy, based on the Newton Raphson scheme for solving the ARE which significantly reduce the risk of instability during the computation of the new accommodated controller. One of the lack of this method is that it works only for actuator or component faults.

• Model Predictive Control Approach

MPC can easily solve the reconfiguration problem with little extra effort in comparison with its use for control [185]. MPC refers to a class of algorithms which make explicit use of a system model to optimize the future predicted behaviour of a plant. At each sampling time t, a finite time optimal control problem is solved over a prediction horizon N, using the current state $\boldsymbol{x}$ of the system as the initial state. The on-line optimization problem takes account of system

dynamics, constraints and control objectives. The optimization yields an optimal sequence of control inputs, and only the control action for the current time is applied while the rest of the calculated sequence is discarded.

To achieve control reconfiguration after the fault occurrence, using the information from the FDI/FDD unit, it is necessary to update the internal plant model of the MPC controller to reflect the system fault. The solution for the actuator faults is simple; actuator limit and rate constraints can be written as

$$u_i^{min} \leq u_i(t) \leq u_i^{max} \tag{1.164}$$

$$\dot{u}_i^{min} \leq \dot{u}_i(t) \leq \dot{u}_i^{max} \tag{1.165}$$

If the actuator i becomes jammed at position u_i^*, the MPC controller can be easily redefined by changing the constraints on input i to

$$u_i^* \leq u_i(t) \leq u_i^* \tag{1.166}$$

$$0 \leq \dot{u}_i(t) \leq 0 \tag{1.167}$$

As a consequence, the MPC controller will find the optimal control sequence using the fault information within the updated model.

This approach is not limited to linear systems, nonlinear or even hybrid systems can be controlled in principle, thus also reconfigured by means of MPC controller. The major drawbacks are: high computing power requirements which limits the applicability to slow plants, and the requirement to know the reference trajectory. A reduction of the real-time computation requirements for MPC results from multi-parametric extensions to MPC, see the survey of Morari et al. [198] or the recent work of Kvasnica et al. [171], where the affine representation of a MPC feedback law is approximated by a single polynomial.

1.4.2.2 Fault-hiding Paradigm

The fault-hiding paradigm, also known as virtual actuator or virtual sensor paradigm, was mentioned by Steffen [267] and implicitly used before by Looze et al. [179] in the form of LQ weights. This approach is highly advantageous since it aims at applying a minimal change in the control loop when faults occur. Thus, the method uses a single nominal controller, designed for the nominal or fault-free system, which is always present in the closed-loop system.

The key idea is to put a reconfiguration block between the faulty plant and the controller, as depicted in Fig. 1.23, to hide the fault from the controller. Hence the nominal controller may remain in the loop. Therein, $\boldsymbol{u}_c$ and $\boldsymbol{y}_c$ are the control input and the plant output seen from the controller, $\boldsymbol{u}_f$ and $\boldsymbol{y}_f$ are the same quantities acting on the plant, $\boldsymbol{d}$ is a disturbance and $\boldsymbol{f}$ represents the faults acting on the plant.

The advantage of this approach is that any existing nominal controller which has been designed, and possibly fine-tuned and tested, to satisfy the desired specifications for the system, can be used and kept in the loop at all times. All algorithms are suitable for online use with problems of medium size (up to 50 states) due to medium computational cost [183]. Both analytical and physical redundancy can be exploited.

All approaches presented in [267] depend on a linearity assumption for the system. Recently, the

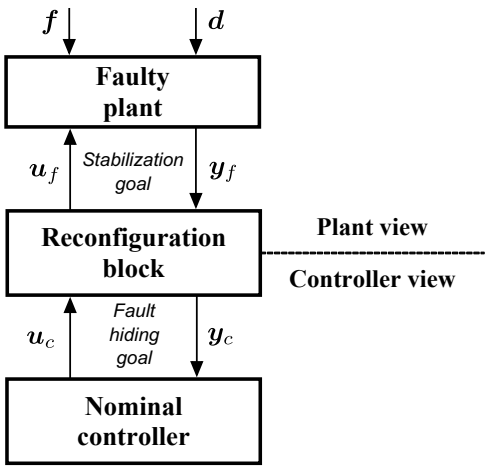


Figure 1.23 – Fault-hiding paradigm scheme

fault-hiding approach has been extended for two classes of nonlinear systems by Richter [250]. For a class of Hammerstein-Wiener's systems, the stability recovery problem after combined actuator and sensor faults has been investigated by Richter [250].

1.4.3 Control Allocation

Control Allocation (CA) is an approach to manage the actuator redundancy in over-actuated systems and is the most famous used for aircrafts, spacecrafts and marine vessels. In the aerospace community, it is probably the most "ready to be implemented" FTC approach. The main reason is that, even if this technique has been used only for a few space experiments[9], the computational complexity is already within the limits of today's off-the-shelf embedded computer systems, see [20, 21, 71, 99, 127, 156, 216, 219]. A recent and complete bibliographical review on CA techniques can be found in [157]. Other reviews can be found in [21, 120, 157]. A comparison study of 16 different CA methods is performed in [219].

The objective of CA is to choose the configuration of actuators to meet a specified objective, subject to saturation and rate constraints (operational ranges of the actuators). In the case of actuator faults, it is desirable to reconfigure the control allocation scheme (re-allocation) in order to make the best use of the remaining healthy actuators [4, 69, 71, 120, 215].

Most CA algorithms assume a linear effector model in the form of a matrix, i.e., a thruster configuration matrix. Thus, control allocation is fundamentally concerned by the inverse computation of the thruster configuration matrix. Since this matrix has more columns than rows (overactuated systems are of interest), there exists an infinite number of solutions. However, by minimizing some "measure" of it, it is possible to have a unique solution. Actuator faults can then be dealt with by control allocation principle so that it is not required to re-design the controller itself (assuming that the CA is feasible to produce the requested control). A consequence is that CA can be used as a FTC solution with a little extra effort on the original techniques. Reference [**?**] also exploits this idea using sliding mode techniques.

[9]For instance, a SIMPLEX–based method is implemented in the ATV developed by EADS Astrium Space Transportation, to carry out a prescribed set of thruster faults.

The following section introduces the main principles of the control allocation technique from a mathematical perspective. Details about implementation issues are given in Chapter 4.

1.4.3.1 The Control Allocation Problem

The concept of CA is to solve undetermined, and typically constrained, systems of equations. The task is to generate the *real control input* $\boldsymbol{u} \in \mathbb{R}^{n_u}$ for the corresponding *virtual control input* $\boldsymbol{v} \in \mathbb{R}^{n_v}$, which is the input of the control allocator. When a set of actuators is actuated by vector $\boldsymbol{u}$, it generates the *total control effort* $\boldsymbol{v}_{sys} \in \mathbb{R}^{n_v}$. If the CA is successful (feasible), then $\boldsymbol{v} = \boldsymbol{v}_{sys}$. Mathematically, for a given $\boldsymbol{v}$, the vector $\boldsymbol{u}$ must be found such that

$$\boldsymbol{h}(\boldsymbol{u}(t)) = \boldsymbol{v}(t) \tag{1.168}$$

where $\boldsymbol{h} : \mathbb{R}^{n_u} \to \mathbb{R}^{n_v}$ is the mapping from the real to the virtual control inputs performed by the actuators and $\text{rank}\big(Jacobian(\boldsymbol{h})\big) = n_v$ [215].

In the literature, the majority of applications considers a linear case. Let's consider a LTI system with n_u inputs

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}_o\boldsymbol{u}(t) \tag{1.169}$$

where the overall input matrix $\boldsymbol{B}_o \in \mathbb{R}^{n_x \times n_u}$ is assumed to have $\text{rank}(\boldsymbol{B}_o) = n_v$. As shown in [119], the input matrix $\boldsymbol{B}_o$ can be factorized as

$$\boldsymbol{B}_o = \boldsymbol{B}_v\bar{\boldsymbol{B}} \tag{1.170}$$

where $\boldsymbol{B}_v \in \mathbb{R}^{n_x \times n_v}$, $\bar{\boldsymbol{B}} \in \mathbb{R}^{n_v \times n_u}$ and both matrices have rank equal to n_v. Now, the total control effort $\boldsymbol{v}_{sys}$, produced by the actuators, is decided by the control effectiveness matrix $\bar{\boldsymbol{B}}$, i.e.,

$$\boldsymbol{v}_{sys}(t) = \bar{\boldsymbol{B}}\boldsymbol{u}(t) \tag{1.171}$$

The control law $\boldsymbol{v}$ is designed based on the pair $(\boldsymbol{A}, \boldsymbol{B}_v)$. Each actuator is assumed to be physically limited by upper and lower position limits, so it is required that

$$u_i^{min} \leq u_i(t) \leq u_i^{max}, \;\; i = 1, \ldots, n_u \tag{1.172}$$

If actuator rate constraints also exist, it is further required that

$$\dot{u}_i^{min} \leq \dot{u}_i(t) \leq \dot{u}_i^{max}, \;\; i = 1, \ldots, n_u \tag{1.173}$$

When a digital controller is used, the rate constraint can be threaded as a time-varying position constraint to adjust "how far can the actuator move during the next sampling period". This results in the following constraint formulation

$$u_i^{min}(t) \leq u_i(t) \leq u_i^{max}(t), \;\; i = 1, \ldots, n_u \tag{1.174}$$

Equation (1.171) constrained by (1.172) and (1.173) (or by (1.174)) constitute the standard formulation of the linear CA problem. Solving this problem might result in three possible situations:

- If $n_v < n_u$ there is an infinite number of solutions. This is the overactuated case, which can degenerate to the exactly actuated case or eventually to the underactuated case in

presence of faults.

- If $n_v = n_u$ there is only one and unique solution. This represents the exactly actuated case.
- If $n_v > n_u$ no solution exists. There are not enough degrees of freedom in the number of control inputs and so a compromise must be made, for example by minimizing a distance between the required control effort and the effort that can be physically achieved. This becomes a crucial aspect within the FTC setting since this means that the impact of the solution has on the control performance should be perfectly known. For example (e.g., in case of rendezvous corridor).

1.4.3.2 Control Allocation Methods

The proposed methods in literature correspond to different ways of computing the solution for a certain CA objective, rather than for different objectives. The most common approaches are the following.

- **Optimization-based methods:** These methods rely on the following pragmatic interpretation of the control allocation problem: given a virtual control command $\boldsymbol{v}$, the goal is to determine a feasible control input $\boldsymbol{u}$ such that (1.171) constrained by (1.172) and (1.173) (or by (1.174)) yields. If there are several solutions, decide the best one by means of a predefined criteria, e.g., l_2 criteria in order to minimize the mean energy consumption, l_∞ criteria to minimize the peak energy consumption. If there is no solution, resolve $\boldsymbol{u}$ such that $\bar{\boldsymbol{B}}\boldsymbol{u}$ approximates $\boldsymbol{v}$ as well as possible [120], e.g., by means of a norm.
- **Direct control allocation:** Here, the choice of control input is made using the knowledge of the geometry of the actuators. This method was firstly introduced by [71].
- **Daisy Chain control allocation:** The allocator suite is divided into groups which are successively employed to generate the total control effort [30]. It can prevent the use of certain actuators until all other actuators have saturated [120].

In the quadratic programming approach to CA, also known as l_2-optimal CA, the control allocation problem is threaded as the following Sequential Least-Squares (SLS) problem

$$\begin{aligned} \mathcal{M} = \arg\min_{\boldsymbol{u}} \|\boldsymbol{W}_v(\bar{\boldsymbol{B}}\boldsymbol{u} - \boldsymbol{v})\|, \quad \text{s.t. } \boldsymbol{u}^{min} \leq \boldsymbol{u} \leq \boldsymbol{u}^{max} \\ \boldsymbol{u}^\star = \arg\min_{\boldsymbol{u}\in\mathcal{M}} \|\boldsymbol{W}_u(\boldsymbol{u} - \boldsymbol{u}_d)\| \end{aligned} \tag{1.175}$$

The above optimization problem (see Fig. 1.24 for an illustration when $n_u = 2$) should be interpreted as follows: given $\mathcal{M}$, the set of feasible control inputs that minimize $(\bar{\boldsymbol{B}}\boldsymbol{u} - \boldsymbol{v})$ (weighted by $\boldsymbol{W}_v$), pick the control input that minimizes $\boldsymbol{u} - \boldsymbol{u}_d$ (weighted by $\boldsymbol{W}_u$). Here, $\boldsymbol{u}_d$ is the desired control input and $\boldsymbol{W}_u$ and $\boldsymbol{W}_v$ are weighting matrices. The weighting matrix $\boldsymbol{W}_u$ gives some specific priority to the actuators and $\boldsymbol{W}_v$ affects the prioritization among the virtual control components when $(\bar{\boldsymbol{B}}\boldsymbol{u} - \boldsymbol{v})$ cannot be attained for example due to the actuator constraints.

If no actuator constraints exist, the above optimization problem has a unique and closed form solution in the least square sense, see Appendix A.3.2. If, however, actuator constraints are

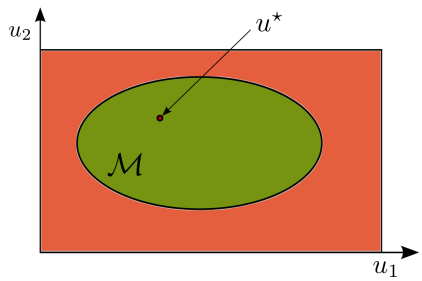


Figure 1.24 – The SLS optimization problem

present, the problem (1.175) can be reformulated into a Weighted Least-Squares (WLS) problem according to

$$\boldsymbol{u}^* = \min_{\boldsymbol{u}} \left(\|\boldsymbol{W}_u(\boldsymbol{u} - \boldsymbol{u}_d)\|^2 + \gamma \|\boldsymbol{W}_v(\bar{\boldsymbol{B}}\boldsymbol{u} - \boldsymbol{v})\|^2 \right), \quad \text{s.t. } \boldsymbol{u}^{min} \leq \boldsymbol{u} \leq \boldsymbol{u}^{max} \tag{1.176}$$

As γ goes to infinity, the two formulations have the same optimal solution $\boldsymbol{u}^*$.

The MATLAB® implementations of the Quadratic Programming Control Allocation Toolbox (QCAT) provides a number of algorithms for control allocation that can be found in the literature [21, 25, 31, 71, 121, 122, 180, 236, 286]. Seven different solvers, suitable to solve the CA problems dealt with in this thesis, have been selected:

SLS Active set solver for the sequential least-squares formulation above. This algorithm determines the optimal solution in a finite number of iterations [122],

MLS Active set based solver for the SLS problem reformulated as a minimal least-squares problem. A limitation is that $\boldsymbol{W}_u$ is required to be diagonal [180],

DIR Direct control allocation solver is based on a simple algorithm which differs from the SLS and WLS formulation. The idea is to determined $\boldsymbol{u}$ such that the two vectors $\bar{\boldsymbol{B}}\boldsymbol{u}$ and $\boldsymbol{v}$ are exactly collinear and their magnitude is as close as possible [21],

WLS Active set based solver for the weighted least-squares formulation. It is based on an algorithm determining the optimal solution in a finite number of iterations [122],

IP Interior point solver for the WLS formulation. Uniform convergence to the optimum in the number of iterations is established in [236],

CGI Heuristic method solver based on cascading generalized inverses (or redistributing pseudo-inverses) for the SLS formulation. It is based on an algorithm requiring only a finite number of iterations but not guaranteing that the optimal solution is found [25, 286],

FXP Fixed-point iteration solver for the WLS formulation. It is based on an algorithm converging to the optimal solution as the number of iterations goes to infinity [31].

The above solvers have been implemented by Härkegård [120] into the QCAT toolbox and will serve as a benchmark in order to compare the results with CA approach proposed in Chapter 4.

1.4.3.3 Control Allocation for Fault-tolerant Control

In order to make use of the remaining healthy actuators in case of actuator faults, it is required to reconfigure the control allocation scheme (re-allocation) by including the constraints due to the faults. As a consequence, the CA principle will find the optimal control combination using the fault information. This means that a FDI or a FDD unit should be joined with the CA algorithm in order to identify the faulty situation. This principle is illustrated in Fig. 1.25.

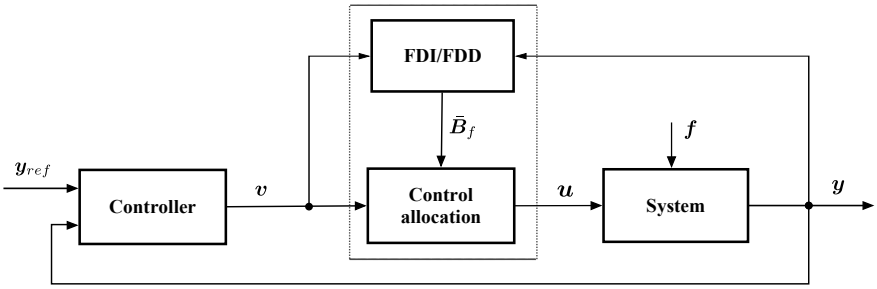


Figure 1.25 – Control allocation scheme

As it can be seen on this figure, the control allocation module takes as inputs the desired virtual signal $\boldsymbol{v}$ and an estimation $\bar{\boldsymbol{B}}_f$ of the actuator configuration matrix $\bar{\boldsymbol{B}}$. This matrix is provided by the FDI/FDD module. Thus, the CA module has the ability to adapt the available actuators to the faults that have occurred. For example, if the effectiveness of a certain actuator becomes 0% due to a fault, the corresponding column in $\bar{\boldsymbol{B}}_f$ becomes $\mathbf{0}$. This actuator is then not considered anymore by the CA algorithm. The goal is then to produce the desired virtual signal $\boldsymbol{v}$ by selecting the appropriate actuator inputs $\boldsymbol{u}$ without considering the faulty actuator. Whether this can be done depends on the situations discussed previously in Section 1.4.3.1, i.e., $n_v < n_u$, $n_v = n_u$ or $n_v > n_u$.

In terms of control re-allocation techniques, a method based on a PIM and fixed-point algorithm (FXP) were proposed and evaluated for a realistic and nonlinear ADMIRE aircraft model in [313]. An on-line sliding mode control allocation scheme for FTC has been developed in [4]. In [72], the problem of CA with magnitude and rate limits on the actuators is considered. The method proposed in [314] looks at restoring as much as possible the performance of the original $\bar{\boldsymbol{B}}$ matrix after an actuator fault. In [162], the integration of reliability indicators into the CA framework was considered.

One of the major advantages of the control re-allocation is that the controller itself does not have to be modified, since it does not change the closed-loop dynamics of the system, assuming that it is feasible to produce the requested virtual control input. However, there are two major limitations to this approach. Firstly, the dynamics and limitations of the actuators after a fault are not taken into account in the control law. This means that the controller will still attempt to achieve the nominal system performance even though the actuators are not able of achieve it. Secondly, there is no guarantee of stability, even with a stabilizing control law, when $n_v > n_u$, as the input seen by the system may not be equal to that intended by the controller [69]. A counterpart of this aspect is that, when there exists redundancy in the actuators, CA technique succeeds and the stability follows. That is why industrials from the space community design their spacecraft with redundant thrusters. It allows, for instance, to guarantee tolerance to

thruster faults.

Note that one of the useful functionality of the CA theory for FTC is the possibility of visualizing the feasible virtual control set $\mathcal{V} = \{\boldsymbol{v} : \boldsymbol{v} = \bar{\boldsymbol{B}}\boldsymbol{u}, \forall \boldsymbol{u} \in \{\boldsymbol{u}^{min} \leq \boldsymbol{u} \leq \boldsymbol{u}^{max}\}\}$ allowing one to prior analyze the fault recoverability/compensability property that is the possibility of the remaining fault free actuators to recover/compensate the fault. This becomes a crucial aspect from a practical point of view and leads the CA technique to be suitable for FTC solutions in spacecrafts.

1.4.4 Enhanced and New Theories in FTC

In this section, two different approaches are briefly introduced to tackle some limitations of the methods described in the previous sections. These two approaches are however out of scope of this thesis.

1.4.4.1 The Supervisory FTC Approach

The major limitations of the classical FDI/FTC methods are: *i*) the problem of guaranteeing stability and performances of the overall FTC scheme taking into account the FDI, the switching and the re-configuration mechanisms is less considered even if it is an important aspect outlined by many authors. In other words, the majority of existing FTC approaches are built on the assumption that each individual unit is assumed to operate correctly, i.e., its output is instantaneously available to provide decisions and/or actions to other subsystems. From a practical point of view, the coupling properties are studied only by means of a Monte Carlo campaign. *ii*) as a direct consequence, even if the stability can be ensured, there exists no direct proof of global optimality of the FTC scheme since the controllers and the FDI/FDD schemes are designed separately.

The method proposed by Efimov et al. [80] deals with the above limitations, particularly:

- Formal stability proofs are established for the overall FTC scheme taking into account the plant model switching, the control reconfiguration switching and the influence of uncertainties and unknown inputs.
- The method allows to design both the FDI and FTC unit taking into account their coupling. Further, it allows to derive a global FDI/FTC scheme with guarantee of stability and well established performance in terms of robustness, fault detection and tolerance.
- Finally, it is proved that the global stability of the FTC system is preserved even if the FDI scheme fails to identify the correct fault. In this case, a system chattering effect may exist that can be reduced by choosing some adequate parameters.

The proposed technique addresses the FDI/FTC design problem for uncertain LTI systems under arbitrary faults since a fault is considered to be a system operating mode. It is assumed that faults cause either instability or performance degradation of the nominal (already in-place) control law, so that the activation of a new controller is required. The main problem is the relation between the fault detection and isolation time and the reconfiguration time so that it is required to detect the smallest possible fault and to accommodate it in an earlier way.

The FTC design problem is formulated within the supervisory framework. The structure of the supervisory FTC architecture that is proposed in [80] is shown in Fig. 1.26.

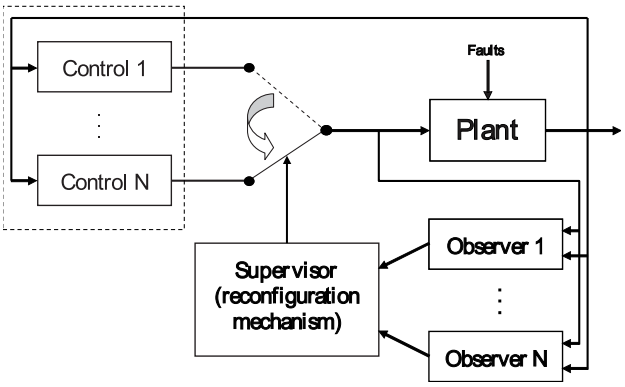


Figure 1.26 – The structure of the supervisory FTC architecture

The supervisor is based on the switching logic that is a decision map $\mathcal{H} : \mathbb{R}^{n_u} \times \mathbb{R}^{n_y} \times \mathbb{R}^{n_x \times N} \to \mathcal{I}$ generating the switching signal

$$\sigma(t) = \mathcal{H}(\boldsymbol{u}, \boldsymbol{y}, \boldsymbol{z_1}, \ldots, \boldsymbol{z}_N) \tag{1.177}$$

which assigns the control algorithm. In ideal case, the control index matches the plant one ($\sigma(t) \to i$). The supervisor has to ensure right continuity of the signal σ, i.e., the signal has to be piecewise continuous and between any two jumps a time delay should exist. The design of the map $\mathcal{H}$ differs depending on the operation conditions. Then, a converging observer exists that solves the detection problem. Typically in the FTC theory these blocks are designed independently, optimizing some performance functionals. As it is well known, the optimality of the subsystems does not imply the same property for the whole system. In the proposed method the optimal properties are critically dependent on switching and, hence, on the supervisor.

The main advantage of the method proposed in [80] is concerned by an approach oriented on the mutual performance optimization of this switched system. For this purpose, the method chooses a characteristic of the hybrid system to be optimized in parallel with the conventional ones used for the observer and the control design. The criterion to be minimized is the minimal admissible time between switches among controls. It is well known that switching among stable linear systems does not lead to instability if the delay between switches are big enough (the minimum delay between switches is called dwell-time). This is why the strategy oriented on this delay increasing is frequently applied in practice to ensure stability in switched systems. However, for FTC systems such approach is not admissible, since it results in an increasing time of reconfiguration, which is dangerous if another fault would appear. This is especially the case for the intermittent faults where the dwell-time value has to be at least smaller than the time variation of two successive faults. Additionally, it may lead to a longer period of wrong control activation for the faulty plant. The both properties are inadmissible for the FTC systems from a practical point of view. Thus, the minimization of the dwell-time value for the supervisory FTC system has to be carefully adequate.

Stability theorems and corollaries are established for both constant and time varying plant index $i \in \mathcal{I}$. The influence of the dwell-time value on the overall system performance is evaluated and a computation procedure for verification of the stability conditions and of the FTC system

synthesis is formulated as a global optimization problem. Norms are used to formulate the problem, but others criteria can be used since the procedure involves a general formulation of a multi-objective optimization problem whereby the choice of the designed parameters is guided by the Pareto optimal points.

Remark 1.20. *An alternative to the dwell-time theory to solve the supervisory-based approach is to use the so-called falsification theory [58, 253–255]. However, as it is proved in [80], the case of the supervisor* (1.177) *involves some restrictive conditions when analysing the stability property of the overall FTC scheme. Thus, the falsification supervisory approach is thought by Efimov et al. [80] to be not a viable candidate for practical FTC solutions.*

Remark 1.21. *Another solution that aims at proposing an enhanced FTC scheme under global stability is the so-called backstepping approach for fault tolerance [154, 292, 293, 320]. However, at this time, only preliminary results exist and the advantage and the application of the method is not well established.*

1.4.4.2 The Trajectory Re-planning Approach

Whatever the selected FTC strategy, a fault cannot be accommodated without sufficient resources in the system. The majority of the existing FTC methods continue to force the system to follow the pre-fault trajectories without considering the reduction in available control resources caused by actuator faults. Forcing the system to follow the same trajectories as before fault occurrence may result in actuator saturation and system's instability. Pre-fault objectives should be redefined in function of the remaining resources to avoid potential saturation. Any reference generation technique can be potentially used. However, in the context of trajectory re-planning for FTC, it is of prime interest to consider the reduction in available control resources caused by the faults.

For systems with input and/or state related constraints, a reference governor or reference management is proposed in the literature. In [13], a command governor based on tools of predictive control is designed for solving set-point tracking problems wherein pointwise-in-time input and/or state inequality constraints are present. A reference governor is designed in [108] for general discrete-time and continuous-time nonlinear systems with uncertainties. It relies on safety properties provided by sub-level sets of equilibria-parameterised functions. In the context of FTC, a reference input management is introduced in [311] to determine appropriate reference inputs in the presence of actuator faults to avoid potential saturation. The idea is to determine the relationship between the closed-loop control signals and the associated reference inputs at steady state and to translate the limits of actuator saturation to the desired requirements on the reference inputs. An on-line adjustment strategy of reference input trajectories is developed using MPC techniques in [278]. Another reference input generation method is proposed using feedback linearization in [54]. The reference input generation, which leads the damaged system to its optimal operating point, corresponds to a nonlinear quadratic programming optimisation problem. The objective is to minimise the distance between the desirable output vector before and after failure occurrence while distributing most equitably the energy among the healthy actuators.

Chamseddine et al. [35] established a relation between the reference trajectory to follow and the remaining resources after fault occurrence. In their work [35], a flatness-based trajectory planning/re-planning method that can be combined with any active FTC approach is proposed.

The work considers the case of over-actuated systems where a new idea to evaluate the severity of the occurred faults is proposed. In addition, the trajectory planning/re-planning approach is posed as an optimisation problem based on the analysis of attainable efforts domain in fault-free and fault cases.

The proposed approach in [35] is applied to two satellite systems in rendezvous mission. The flatness-based trajectory planning/re-planning approach is formulated as an optimisation problem to minimise the total time $(t_f - t_0)$ of the mission while avoiding hitting actuator constraints, i.e.,

$$\begin{cases} \text{Minimise} & t_f - t_0 \\ \text{Subj. to} & \|\boldsymbol{v}^*(t) - \boldsymbol{c}\| < \rho^2 R^2, \ \ \forall t \end{cases} \tag{1.178}$$

where t_0 is the initial and t_f the final time of the mission, and $\boldsymbol{v} \in \mathbb{R}^{n_v}$ is the vector of desired efforts (the application of [35] considers only the position dynamics, i.e., $n_v = 3$). The parameters $\boldsymbol{c} \in \mathbb{R}^{n_v}$ and $R \in \mathbb{R}^+$ are used to determine a sphere $\mathcal{S}$ with a center $\boldsymbol{c}$ and radius R. This sphere is the largest sphere included in the set of attainable efforts $\Phi = \{\boldsymbol{v} \in \mathbb{R}^{n_v} : \boldsymbol{v} = \bar{\boldsymbol{B}}\boldsymbol{u}, \forall \boldsymbol{u} \in \Omega\}$, where Ω stands for the set of attainable control inputs $\boldsymbol{u}$ and $\bar{\boldsymbol{B}}$ is the actuator effectiveness matrix. The parameter $0 < \rho < 1$ is used to consider model uncertainties. The desired effort $\boldsymbol{v}^*(t)$ can be generated by the control inputs $\boldsymbol{u}$ if $\boldsymbol{v}^*(t) \in \Phi$. If the optimization problem (1.178) is feasible, then $\boldsymbol{v}(t)^* \in \Phi, \forall t \in [t_0, t_f]$ since $\mathcal{S} \subseteq \Phi$. When actuator faults occur, the set Φ shrinks. The idea of the proposed method is to use the reduction in the domain Φ (and thus of $\mathcal{S}$) to evaluate the severity of faults.

The major limitations of this approach is that the obtained trajectories are suboptimal since the reference trajectories are restricted to polynomial functions of time (Bézier polynomial functions of degree three) leading to a less smooth control efforts. Moreover, the set of attainable control efforts is approximated by a spherical subset and a perfect FDI unit is assumed (detection/isolation delay and the coupling between the FDI and FTC units are not addressed).

1.5 Conclusion

In this chapter, the state of the art of the main model-based FDI/FDD and FTC techniques has been presented. Bibliographical references are given for the main contributions. Some application examples from aerospace field have been introduced to highlight the applicability of the selected methods. In the following, a summary of the previously introduced FDI/FDD and FTC techniques is given in tabular forms. The next chapters address the main content and contributions of the work presented in this thesis.

1.5.1 Summary of the FDI/FDD Approaches

It is believed that the described FDI/FDD methods can also be classified according to seven criteria (see below) which lead to the classification proposed in Table 1.2.

1. Detection Time Performance (DTP) measure, defined as the time to detect (detection delay) normalized with respect to the maximum allowed time to detect. Statistics of this index, such as mean, minimum and maximum values, variance, etc., can for example be used with respect to the number of Monte Carlo (MC) runs.

2. The missed detection rate, which is a ratio of missed fault cases with respect to the total number of MC runs,
3. The false alarm rate, which is the ratio of false alarm cases with respect to the total number of MC runs without faults.
4. The executive time (in number of processor cycles), allowing the required executive time to be measured once a FDI design is coded using a oriented processor language.
5. The tuning complexity index, which is a metric allowing the re-use capacity of the FDI technique to be measured from a user point of view. It includes the number of input parameters to tune for a given scenario (e.g., the dimension of the $\boldsymbol{Q}$ and $\boldsymbol{R}$ matrices for a Kalman Filter-based algorithm).
6. The "formal proof for performance" criterion. This criterion indicates if there exists a formal proof of a given FDI algorithm to cover a specified set of faults.
7. Finally, the last criterion aims at quantifying if an FDI technique is suitable for FTC approaches described in the next section.

These metrics allow the existing approaches (described in this thesis) to be easily compared in terms of application criteria. The signs indicate that an approach fulfils a requirement very well (++), well (+), in a limited fashion (0), not favorable (-) or not applicable (--).

1.5.2 Summary of the FTC Approaches

With respect to the AFTC approaches, an attempt was made to do a classification that can be a be a possible guideline to choose the adequate solution for a given problem. This classification can be found in Table 1.1. In this table, the explanation of the signs corresponds to the ones presented in Table 1.2.

Note that since FTCS design is a recent topic in the research community, there is lack of a clear and recognized classification. There only exist some disseminate studies and applications. Especially in terms of space applications, there only exist a few published papers.

Table 1.1 – Classification of the introduced AFTC approaches

Method/Criteria	Reusable	Tuning complexity	On-line solution	Guaranteed stability	Computational burden
MMST	+	+	--	0*	++
IMM	+	++	-	+*	++
Bank of observers	+	+	+	0*	0
PIM	+	0	+	--*	+
Modified PIM	+	0	++	++*	-
Admissible PIM	+	+	++	++*	+
EA	+	+	++	++*	-
Model following	++	+	++	+*	0
LQ-redesign	+	++	+	+*	-
MPC	++	++	++	+*	-
Fault hiding	++	+	+	+*	0
CA	++	++	++	+	0

*These techniques have been studied only under the assumption of perfect FDI which is though a negative aspect since the global stability of the overall FTC scheme (i.e., taking into account the FDI unit performance) cannot be formally proved.

Table 1.2 – Classification of the existing FDI approaches

Criterion/ Method	DTP (mean, max, variance)	Missed detection rate	False alarm rate	Executive time	Tuning complexity	Formal proofs for performance	Suitability for FTC
Parity Space	++:static approach ---:dynamic approaches not really evaluated	Highly depend on measurement noise	Highly depend on the measurement noise	++:dynamic and static approaches	++:dynamic and static approaches	--:requires a MC campaign	++:for sensor faults -:not really evaluated
Iterative Learning Observer	N/A	N/A	N/A	0	+	-:MC campaign is preferable -:MC campaign to tune the decision algorithm	+
Unknown Input Observer	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++	+:may exist difficulties for determination of the disturbance matrix effect	++:when faults behave in a different space of disturbances to be decoupled --:otherwise -: MC campaign to tune the decision algorithm	++
Eigenstructure Assignment	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++	+:may exist difficulties for determination of the disturbance matrix effect	++:when faults behave in a different space of disturbances to be decoupled -:otherwise -:MC campaign to tune the decision algorithm	++
Sliding Mode Observer	++	++	++	--:very time consuming	-:many parameters may be involved	+:in terms of stability and robustness --:requires a MC campaign for sensitivity -:MC campaign to tune the decision algorithm	+:very suitable for dynamic control allocation
Parameter Estimation (KF, EKF, UKF, Particle Filtering)	+:difficulties in the problem formulation (what kind of parameters to estimate?)	+:difficulties in the problem formulation (what kind of parameters to estimate?)	+:difficulties in the problem formulation (what kind of parameters to estimate?)	-:KF --:EKF, UKF, Particle Filtering	--: the tuning parameters (covariance matrices) are very hard to relate with physical properties	-:MC campaign is preferable -:MC campaign to tune the decision algorithm	++:very suitable for dynamic control allocation
Norm-based (H_2,H_∞, H_∞/H_-)	++	++	++	++: the filter can be converted to discrete time very easily	+:weighting functions are related to frequency specifications	++:stability and sensitivity is proved -:H_2 criteria is useless -:MC campaign to tune the decision algorithm	0:not yet well established
Geometric approaches	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++:when faults behave in a different space of disturbances to be decoupled -:otherwise	++	+:may exist difficulties in the problem formulation	-:MC campaign is preferable -:MC campaign to tune the decision algorithm	--

Chapter 2

MSR Mission Description and Modelling

"We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard!"
— John F. Kennedy, American president

This chapter describes the Mars Sample Return (MSR) mission, its rendezvous phase and the vehicles involved (i.e., the target and chaser spacecraft) in the mission. It describes the Guidance Navigation and Control (GNC) unit that is in charge of controlling the chaser during the rendezvous phase and the failure management unit that is in charge of detecting failures and of engaging corrective maneuvers. It is shown how the FDIR and FTC solutions investigated in the next chapters, can be integrated in the failure management unit. This chapter also addresses the models of the chaser spacecraft dynamics (relative position between the chaser and the target and chaser attitude) that will be further used in the following chapters to design model-based FDIR/FTC solutions. Modelling of the chaser spacecraft thruster-based propulsion is also addressed to outline the effect of the faults. The considered fault scenarios are also discussed. It should be outlined that the work presented in this thesis does not consider the solar panel flexible modes, the slosh phenomena and the time-variations of the center of mass (it considers uncertain center of mass) of the chaser spacecraft. These problems are currently studied within the iGNC project (Integrated GNC Solutions for Autonomous Mars Rendezvous and Capture), see [213, 240].

2.1 Overview of the MSR Mission

The Red Planet has been an object of fascination and mystery since ancient times and still remains a primary goal for space robotic explorations. Rovers and other space vehicles do a great job studying Martian geological structures and biology. However, bringing samples of Mars back to Earth is still challenging for answering critical scientific questions that cannot be addressed by purely "in situ" missions, where it is not possible to effectively use the large international capabilities in scientific instrumentation.

The Mars Sample Return mission is one of the most exciting challenges in the international

effort on the Solar System exploration. The mission concepts have been studied for years by NASA (D'Amario et al. [53]), French National Space Agency (CNES) (Cazaux et al. [34]) and ESA. Its main goal is to collect samples of Martian rocks, soils and atmosphere, and to return these samples safe and intact back to Earth for analysis. The importance and complexity of this mission calls for a global effort, with particular collaboration between ESA and NASA, as well as the participation of other space agencies [82].

The mission consists of two spacecrafts directly injected towards Mars by launchers [11]. The descent module is released on the Martian atmosphere (Entry phase), lands on the Mars surface and a Mars rover vehicle is released. Once the rover finished the collecting procedure, the samples are put into the sample container and loaded on the Mars Ascent Vehicle (MAV) which is then launched, by means of rockets, into a low Mars orbit. Meanwhile the second module, the rendezvous system (chaser) and the Earth Re-entry Capsule (ERC), is injected towards the Mars planet to rendezvous with the sample container (target) and bring it back to Earth. The chaser achieves the sample capture as soon as it is released by the MAV, which performs the last maneuver in order to avoid any interference with the rendezvous operation. Finally, after successful capture, the sample container is inserted into ERC inside the chaser vehicle and the chaser starts its interplanetary cruise towards the Earth. Figure 2.1 provides an overview of the mission.

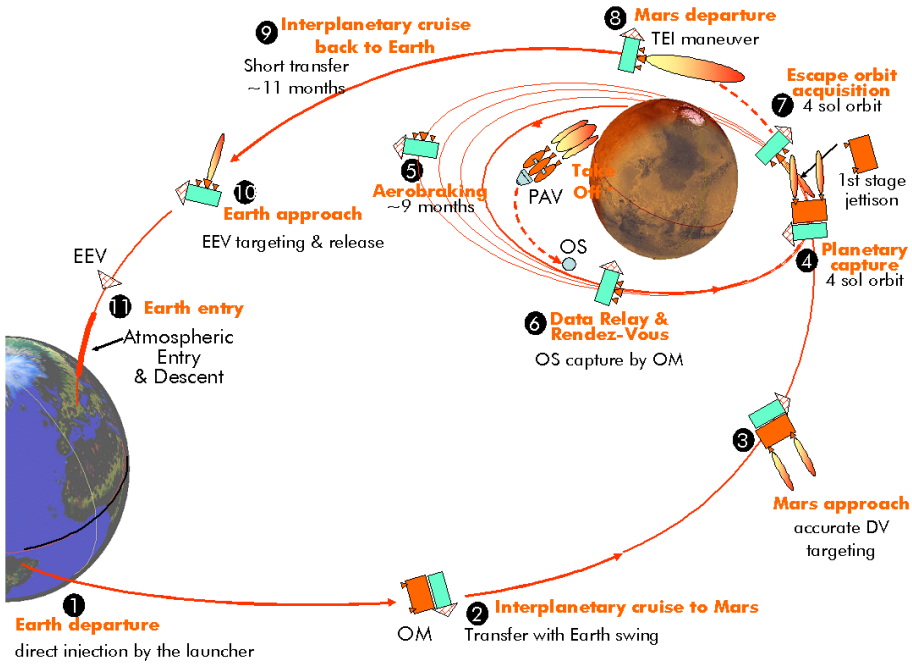


Figure 2.1 – Illustration of the principal steps of the MSR mission, ©2012 TAS

The target is a diameter spherical container whereas the chaser capture mechanism is a basket with cylindrical aperture which is part of the sample handling system. During the capture, the chaser aperture must face towards the target. The objective is obviously to successfully capture the target. To achieve this, the capture conditions in terms of position and velocity, and of attitude error and angular rates must be achieved within a certain precision, see Table 2.1 for numerical values of the considered capture requirements. These values are driven by the capture mechanism.

Capture condition		Nominal value	Max variation	Unit
Translational conditions	Position misalignment on +X face	0.0	0.20	m
	Longitudinal X velocity accuracy	0.1	0.05	m/s
	Lateral Y and Z velocity error	0.0	0.04	m/s
Rotational conditions	Angular rate error	0	$0.3^\star$	deg/s
	Angular misalignment	0	$2^\star$	deg

Table 2.1 – MSR conditions for successful capture (* are 3σ requirements)

In terms of mission performance, the critical constraints are the size of the approach corridor driven by the light detection and ranging (LIDAR) sensor field of view and the velocity profile of the chaser (the capture should be done at velocity very close to zero). Therefore, during the whole rendezvous phase, the chaser spacecraft must maintain its trajectory inside the rendezvous corridor (see Fig. 2.17 for an illustration), its velocity along the capture axis is close to 10 cm/s for capture, and must keep its attitude pointing towards the target with maximum attitude misalignment of 20° on all the three axis. The minor objective for the rendezvous problem is to minimize the fuel consumption.

A number of new technologies are required to successfully accomplish this pioneering mission. One of them is the rendezvous and capture system, which will be able to detect, approach and capture the sample container, previously put in a predefined orbit by the MAV. See Fig. 2.2 for an illustration.

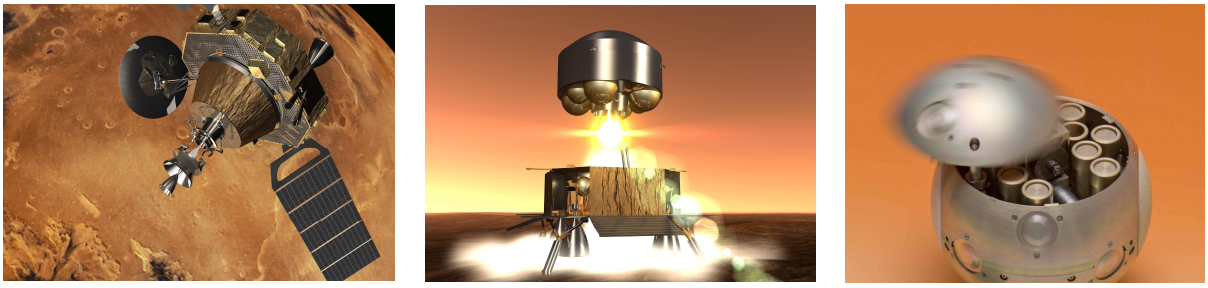


Figure 2.2 – Artist's view of the chaser spacecraft (left) and of the Mars ascent vehicle (middle) lifting off from Mars surface with the Martian soil samples (right), ©2006/2013 ESA

2.1.1 Terminal Rendezvous Phase

The mission scenario considered in this thesis corresponds to the last twenty meters of the rendezvous phase, where the target vehicle, containing samples from the Mars surface, has to be successfully captured by the controlled spacecraft (chaser). The terminal rendezvous/capture phase starts at the point (final holding point) where the chaser has been brought into approximately the same orbit as the orbit of the target, i.e., approximately 20 m from the target. The initial conditions, expressed in terms of Keplerian orbital elements [89, 197, 259] are enumerated in Table 2.2.

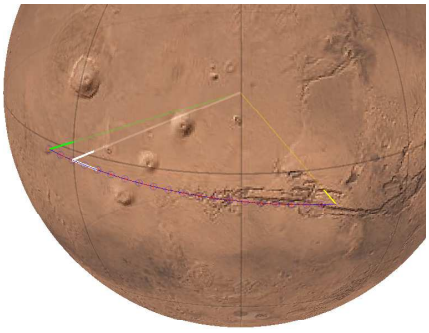


Figure 2.3 – Mars rendezvous orbit

Orbital parameter	Chaser	Target	Unit
Semimajor axis	3893	3893	km
Eccentricity	0	0	n/a
Inclination	30	30	deg
RAAN	0	0	deg
Argument of periapsis	0	0	deg
True anomaly	-32.16×10^{-5}	0	deg

Table 2.2 – Keplerian orbital parameters (initial) of the chaser and target

Here, the guidance law is tasked with accelerating the chaser to reach the required velocity profile (10 cm/s) and with moving the chaser to a position of 3 m from the target. At a distance less than 3 m of separation, the remainder of the maneuver is passive (no active position control) and the chaser trajectory shall freely drift upwards to intercept the Y axis. During the whole length of this phase, the chaser must maintain its line of sight pointing towards the target. It is necessary for the short-range relative navigation sensors to function correctly. At the last tenths centimeters, the attitude guidance will align the capture mechanism towards the target. The simulation, however, stops at the point when this phase begins.

Combination of high control accuracy due to the tight capture tolerances together with the distances involved, and the resulting communication delays (up to 20 minutes in each direction), there is a particularly strong motivation to perform this operation autonomously.

2.2 Chaser Spacecraft GNC

The rendezvous GNC unit of the chaser spacecraft corresponds to a 6 Degree of Freedom (DOF) control. It ensures the application of both commanded torque and force using thrusters only. Figure 2.4 shows the general setup of the GNC system of the chaser vehicle.

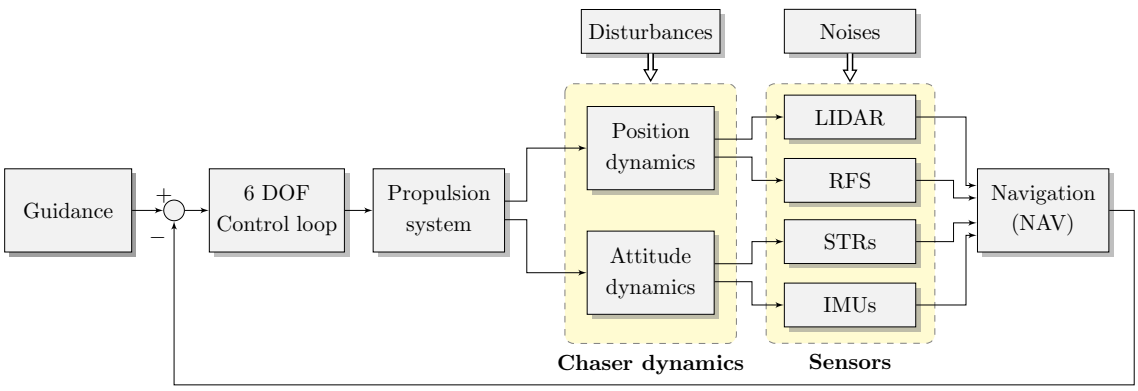


Figure 2.4 – General setup of the chaser's GNC system during the rendezvous

The set of sensors and actuators during the terminal rendezvous is minimized to reduce the risk of fault occurrence and to reduce the power consumption and mass [240]. The control unit during the rendezvous phase relies on a precise on-board sensor systems composed of:

- two 3-axis Inertial Measurement Units (IMUs) in hot redundancy,

- two Star Trackers (STR) in cold redundancy, and
- two short-range rendezvous sensors with a functional hot redundancy:
  - a Light Detection and Ranging (LIDAR) sensor, and
  - a Radio Frequency Sensor (RFS) as back-up.

The IMU is an electronic device that is in charge of measuring the chaser angular velocity $\boldsymbol{\omega} = [p, q, r]^T$ using a combination of accelerometers and gyroscopes, sometimes also magnetometers. The quaternion-producing STR provides the measurement of the (normalized) chaser attitude quaternion $\boldsymbol{q}_c$ which can be easily converted to Euler angles $\boldsymbol{\Theta} = [\varphi\, \theta\, \psi]^T$, see Appendix A.5.2 for conversion details. The LIDAR unit is in charge of the measurement of the relative position $\boldsymbol{\rho} = [\xi\, \eta\, \zeta]^T$ between the chaser and target. The RFS sensor is used to monitor the chaser trajectory, and it can trigger a Collision Avoidance Maneuver (CAM), if necessary.

The role of the navigation unit (NAV) is to perform reliable estimates $\hat{\boldsymbol{q}}_c$, $\hat{\boldsymbol{\Theta}}$, $\hat{\boldsymbol{\omega}}$, and $\hat{\boldsymbol{\rho}}$ of $\boldsymbol{q}_c$, $\boldsymbol{\Theta}$, $\boldsymbol{\omega}$, and $\boldsymbol{\rho}$, respectively, by removing the misalignment phenomena, sensor bias and noises on these measurements. The navigation unit also provides an estimate of the target attitude quaternion $\hat{\boldsymbol{q}}_t$, that will be used later for the design of the FDI unit. It is assumed that the NAV unit is decoupled from thruster faults, but providing "non-perfect" state estimates, i.e., there still exists some unfiltered noises on $\hat{\boldsymbol{\omega}}$, $\hat{\boldsymbol{\rho}}$, $\hat{\boldsymbol{q}}_t$ and $\hat{\boldsymbol{q}}_c$ (and therefore on $\hat{\boldsymbol{\Theta}}$) and also there exists a constant delay between the NAV unit and the controller, see Section 2.2.1 about measurement noise modelling.

In terms of actuators, the chaser spacecraft is equipped with a very precise chemical propulsion system composed of N bi-propellant thrusters.

In this thesis, two distinct thruster configurations with different number of thrusters and different geometrical layout are considered. The properties of these configurations are introduced at the beginning of each chapter where they are considered. The chaser is also equipped with a set of reaction wheels in a classical pyramidal configuration. However they are not used during the rendezvous phase, therefore they are not considered in this thesis and the terms "actuator" and "thruster" are used interchangeably.

Remark 2.1. *In the delivered version of the simulator that was used for all simulations in Chapter 3 and Chapter 4, the NAV block is not modelled and therefore an appropriate model of the coupling between the sensor blocks and NAV is considered. This is the purpose of the next section.*

2.2.1 Sensors and Navigation Modelling Issues

The purpose of this section is to describe the models of the sensors used during the terminal rendezvous phase to capture the target. As explained previously, see Fig. 2.4 if necessary, those sensors are the LIDAR, the STR and the IMU sensors. The case of the RFS is not considered in the following since, again, it is only used to monitor the chaser trajectory and thus is not involved in the control loop. All the sensors, which are a part of the navigation unit too, are assumed to deliver their measures synchronously at sampling frequency of 10 Hz.

2.2.1.1 LIDAR Modelling Issues

Today's modern short rendezvous LIDAR devices dispose of high accuracy level. As such, that most space agencies (NASA, ESA, CNES) have already identified LIDAR as a viable candidate instrument for autonomous rendezvous [172, 235]. It seems to be a justified, precise and robust device for the MSR mission success [200]. Therefore, all along this thesis, the LIDAR model is assumed to correspond to a perfect measure corrupted by an error. This error is assumed to be an additive zero-mean Gaussian white noise, i.e.,

$$\hat{\boldsymbol{\rho}}(k) = \boldsymbol{\rho}(k) + \boldsymbol{w}_\rho(k) \tag{2.1}$$

where $\boldsymbol{w}_\rho \in \mathbb{R}^3$ is a random process following a normal distribution $\mathcal{N}(0, \sigma_\rho^2)$.

High demand is put on the LIDAR to meet the navigation accuracy required for a close range rendezvous. This motivated some researchers to consider a relatively small noise variance for this device [123, 261]. In this work, the corresponding 3-sigma values are $3\sigma_\rho = 0.035/\sqrt{2}$ (m) for all three axes (ξ η ζ).

Remark 2.2. *Despite the fact that the velocity measurements are not used in any of the proposed FDI/FTC schemes developed in this thesis, the same noise model was assumed for the velocities (used by the nominal controller) with the following 3-sigma values:* 0.009 (m/s) *for* $\dot{\xi}$ *axis and* 0.007 (m/s) *for the remaining two axes* $\dot{\eta}$ *and* $\dot{\zeta}$*, respectively.*

2.2.1.2 Attitude Quaternion Modelling Issues

The STRs are in charge to deliver the attitude quaternion. The model considered in this thesis corresponds to the perfect quaternion measure corrupted by a noise.

To proceed, let the chaser (or the target) attitude be represented by the unit quaternion (see Appendix A.5 for quaternion definitions and algebras)

$$\boldsymbol{q} = (q_0, q_1, q_2, q_3), \quad \boldsymbol{q} \in \mathbb{H} \quad q \in \{\boldsymbol{q}_c, \boldsymbol{q}_t\} \tag{2.2}$$

satisfying the unity constraint

$$\|\boldsymbol{q}\| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2} = 1 \tag{2.3}$$

Let a random variable $\boldsymbol{w}_q \in \mathbb{R}^3$ follow a uniform distribution $\mathcal{U}(-\mathfrak{u}, \mathfrak{u})$, where $\mathfrak{u} > 0$. The vector $\boldsymbol{w}_q$ can be regarded as a rotation vector. This means, that $\boldsymbol{w}_q$ represents a random rotation with the angle

$$\alpha_w = \|\boldsymbol{w}_q\| \tag{2.4}$$

around the axis

$$\boldsymbol{e}_w = \frac{\boldsymbol{w}_q}{\|\boldsymbol{w}_q\|} \tag{2.5}$$

The quaternion representation $\boldsymbol{q}_w$ of this rotation is

$$\boldsymbol{q}_w = \left(\cos\left(\frac{\alpha_w}{2}\right), \boldsymbol{e}_w \sin\left(\frac{\alpha_w}{2}\right)\right) \tag{2.6}$$

This noise quaternion can be now used to correctly corrupt a deterministic quaternion $\boldsymbol{q}$ (representing the real attitude in our case) to obtain a disturbed quaternion $\hat{\boldsymbol{q}}$, i.e.,

$$\hat{\boldsymbol{q}}(k) = \boldsymbol{q}(k) \odot \boldsymbol{q}_w(k) \tag{2.7}$$

where $\odot$ stands for a quaternion product (see Appendix A.5.3). A noisy quaternion $\hat{\boldsymbol{q}}$ obtained in this way with $\mathfrak{u} = 10^{-4}$ aims to model the imperfections of the sensor/navigation unit when speaking about the target or chaser quaternion. This type of measurement model is often used by the industry to model the coupling between the unmodelled sensor and the navigation blocks. Note, that since both quaternions $\boldsymbol{q}$ and $\boldsymbol{q}_w$ are unit, the resulting quaternion $\hat{\boldsymbol{q}}$ will keep this property too.

2.2.1.3 Angular Rate Measurement Model

Gyros (part of the IMU) are subject to different kind of uncertainties, such as noise and bias. In accordance with the literature [173], a widely used gyro model is considered in this thesis, such as

$$\begin{cases} \hat{\boldsymbol{\omega}}(k) = \boldsymbol{\omega}(k) + \boldsymbol{b}(k) + \boldsymbol{w}_r(k) \\ \dot{\boldsymbol{b}}(k) = \boldsymbol{w}_b(k) \end{cases} \tag{2.8}$$

where $\boldsymbol{b} \in \mathbb{R}^3$ is a slowly varying gyro bias vector, $\boldsymbol{w}_r \in \mathbb{R}^3$ and $\boldsymbol{w}_b \in \mathbb{R}^3$ are independent zero-mean Gaussian white noise processes following a normal distribution $\mathcal{N}(0, \sigma_r^2)$ and $\mathcal{N}(0, \sigma_b^2)$, respectively. The 3-sigma values are $3\sigma_r = 0.0016$ (deg/s) and $3\sigma_b = 0.2282 \times 10^{-5}$ (deg/s^2)

2.2.2 Translation and Attitude Guidance

The guidance function which fundamentally is nothing else than a path planning algorithm, is in charge of generating the position/velocitiy profiles $\boldsymbol{\rho}_r = [\xi_r \ \eta_r \ \zeta_r]^T / \dot{\boldsymbol{\rho}}_r = [\dot{\xi}_r \ \dot{\eta}_r \ \dot{\zeta}_r]^T$ and quaternion attitude/angular velocity profiles $\boldsymbol{q}_r = [q_{0_r} \ q_{1_r} \ q_{2_r} \ q_{3_r}]^T / \boldsymbol{\omega}_r = [p_r \ , \ q_r \ , \ r_r]^T$ for the rendezvous and capture phases. Its function is to provide the reference state vectors as well as to compute and provide any feed forward control signals, if required.

• Position Guidance

In terms of position, the guidance for the final approach consists successively of a station keeping phase, an acceleration part followed by a constant velocity part which corresponds to the final docking velocity and a free drift. Past research has focused on various acceleration profiles to have smooth velocity profiles with indifferent results. The profile used for the terminal rendezvous of the MSR mission between the chaser and the target, is based on having constant accelerations leading to a simple and fast profile. This profile is defined in the local frame $\mathcal{F}_l = \{O_T; \vec{\boldsymbol{X}}_l, \vec{\boldsymbol{Y}}_l, \vec{\boldsymbol{Z}}_l\}$, see Fig. 2.5 for an illustration. This frame is fixed at the center of the target O_T, with its $\vec{\boldsymbol{Z}}_l$ axis be perpendicular to the $\vec{\boldsymbol{X}}_l$ and $\vec{\boldsymbol{Y}}_l$ axis and oriented as shown in Fig. 2.5.

The phase plane profiles for the final approach is illustrated in Fig. 2.6. The guidance profile is generated for each separate segments as illustrated, each segment corresponding to a rendezvous phase. The first segment defined for times $t \in [t_0, t_1]$ corresponds to the station keeping phase,

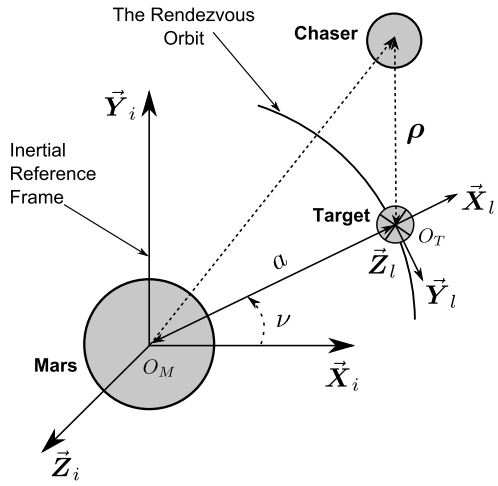


Figure 2.5 – The Mars rendezvous orbit with the associated frames

the second segment $t \in [t_1, t_2]$ refers to the constant acceleration phase, the third segment $t \in [t_2, t_3]$ is the constant velocity phase and finally, the fourth segment $t \in [t_3, t_4]$ refers to the free drift phase. The target is reached at time t_4. Fig. 2.6 illustrates the phase plane profiles along the X and Y axes. The profile along the Z-axis is not presented since it is quite evident: since the rendezvous is done in the X-Y orbit plane, the Z-axis profile has to be fixed to zero. Thus $\zeta_r = 0$ and $\dot{\zeta}_r = 0$. In other words, the guidance profile is specified so that there is no motion in the out-of-plane of the orbit plane.

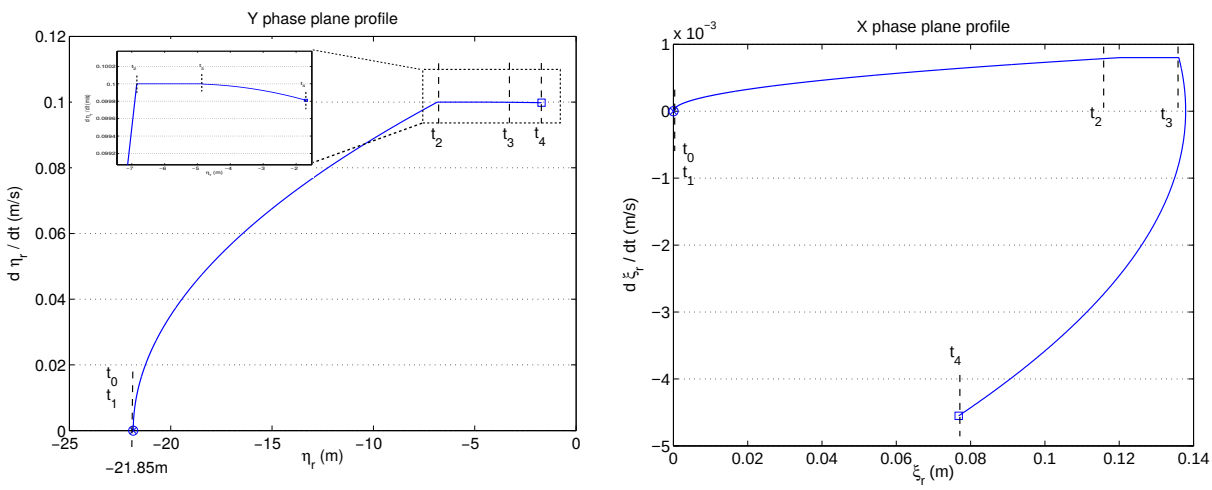


Figure 2.6 – The phase plane profiles for the final approach: Y plane (left) and X plane (right)

During station keeping, i.e., $t \in [t_0, t_1]$, the reference vector signal $\boldsymbol{\rho}_r$ will keep the spacecraft at a chosen location, i.e., the position reference are the coordinates of that point. This point corresponds to the initial position given in the Table 2.2. The reported coordinates are given in the inertial frame $\mathcal{F}_i = \{O_M; \vec{\boldsymbol{X}}_i, \vec{\boldsymbol{Y}}_i, \vec{\boldsymbol{Z}}_i\}$ which is attached to the centre of the Mars O_M, see Fig. 2.5 for an illustration. However, it can be verified that, in the local frame, those coordinates are given according to $\boldsymbol{\rho}_r = [0 \ \ -21.85 \ \ 0]^T$ m. Such coordinates indicate that the chaser is in the same orbit plane of the target but is put behind the target at a distance of 21.85 m. During station keeping, the velocity reference is zero along all axes, i.e., $\dot{\boldsymbol{\rho}}_r = 0$.

For the other segments, it is necessary to find the time $t_i, i = 1, ...4$ and the location $\eta_r(t_i)$ and $\xi_r(t_i)$ at the shift points. Regarding the Y profile, this is all done based on the standard kinematic solution under constant acceleration that can be written in the general form as $s = s_0 + v_0 t + \frac{1}{2}at^2$, where s is the distance, v_0 is the initial speed, and a, the applied acceleration. The following gives the solution of the problem for the constant acceleration phase. The intermediate calculus are omitted since they are well known.

$$\eta_r(t) = \eta_r(t_1) + \frac{1}{2}\ddot{\eta}_0 t^2 \quad \forall t \in [t_1, t_2] \tag{2.9}$$

$\eta_r(t_1) = -21.85$ m being the coordinate of η_r at the end of the station keeping phase and $\ddot{\eta}_0 = 0.33.10^{-3}$ m/s^2 being the required acceleration. The speed is then given by

$$\dot{\eta}_r(t) = \ddot{\eta}_0 t \tag{2.10}$$

The solution of the constant velocity phase is

$$\eta_r(t) = \eta_r(t_1) + \dot{\eta}_r(t_2)(t - t_2) \quad \forall t \in [t_2, t_3] \tag{2.11}$$

the speed being $\dot{\eta}_r(t_2) = 0.1$ cm/s. The last phase (free drift) corresponds to a (progressive) deceleration phase until the target is reached.

$$\eta_r(t) = \eta_r(t_4) - \dot{\eta}_r(t_2)(t_3 - t_2) - \frac{d}{2}(t_3 - t_2)^2 + \dot{\eta}_r(t_2)(t - t_3) + \frac{d}{2}(t - t_3)^2 \quad \forall t \in [t_3, t_4] \tag{2.12}$$

where d refers to the slope of the required deceleration. The X profile (i.e., the definition of $\xi_r(t)$) follows exactly the same principle. Figure 2.7 illustrates the overall profiles in the time domain. The different phases, i.e., station keeping phase for $t \in [t_0, t_1]$, constant acceleration phase for $t \in [t_1, t_2]$, constant velocity phase for $t \in [t_2, t_3]$ and free drift phase for $t \in [t_3, t_4]$, can also be easily identified.

- **Attitude Guidance**

The attitude guidance loop is very simple. Since the navigation unit provides the attitude quaternion of the target $\hat{\boldsymbol{q}}_t$, the attitude guidance loop obeys simply to the rule *"follow the attitude quaternion of the target with a shifted angle for φ equal to 90°"*, i.e.

$$\boldsymbol{q}_r = \hat{\boldsymbol{q}}_t + \boldsymbol{q}_{90^o} \tag{2.13}$$

The reason of the shift of 90° for φ is due to the position of the capture mechanism, i.e., its entry is placed perpendicular to the face of the chaser spacecraft. In this equation, $\boldsymbol{q}_{90^o}$ is the quaternion associated to $\varphi = 90^o$, see Appendix A for quaternion's algebra. The reference angular velocity $\boldsymbol{\omega}_r$ is derived from the relation

$$\begin{bmatrix} \mathbf{0} \\ \boldsymbol{\omega}_r \end{bmatrix} = 2\dot{\hat{\boldsymbol{q}}}_t \hat{\boldsymbol{q}}_t^* \tag{2.14}$$

Figure 2.7 (bottom right) illustrates the attitude profile in the inertial reference $\mathcal{F}_i$. For better understanding, the quaternion $\boldsymbol{q}_r$ is converted into Euler angles φ, θ, ψ. Furthermore, the different shifting points of the position profiles (station keeping for $t \in [t_0, t_1]$, constant acceleration

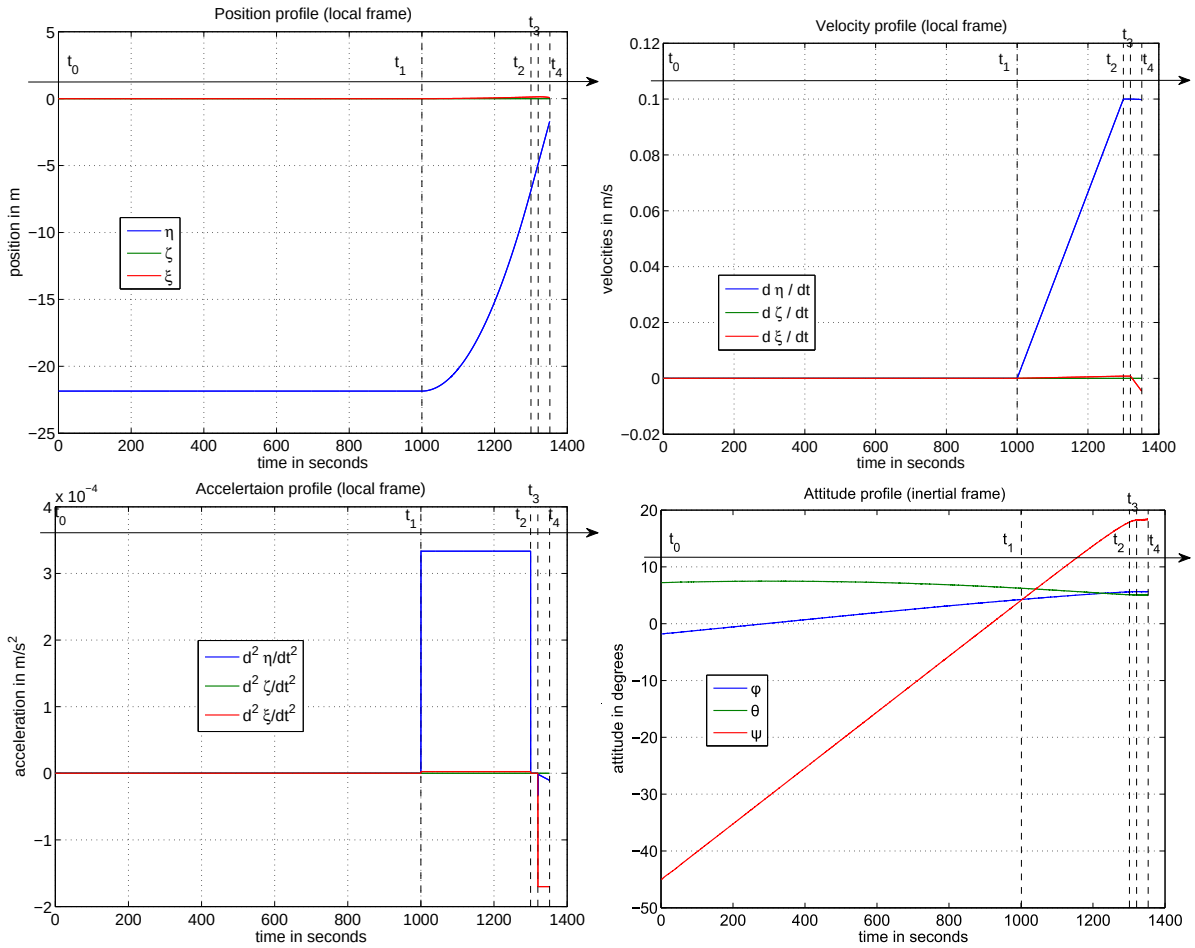


Figure 2.7 – The translation profiles (top and bottom left) and the attitude profile (bottom right) of the guidance loop

phase for $t \in [t_1, t_2]$, constant velocity for $t \in [t_2, t_3]$ and free drift for $t \in [t_3, t_4]$) is reported for better understanding of the coupling between the position and the attitude trajectories.

2.2.3 Control and Actuator Management Functions

To carry out the mission and to ensure the required performance, the chaser spacecraft has a fine 6 DOF manoeuvring capability. This is ensured by a 6 DOF control law whose architecture is illustrated on Fig. 2.8.

It mainly consists of two linear controllers, $\boldsymbol{K}_{pos}$ and $\boldsymbol{K}_{att}$, a Thruster Modulator Unit (TMU) and a Thruster Management Function (TMF). The role of the matrix rotation $\boldsymbol{R}(\hat{\boldsymbol{q}}_c, \hat{\boldsymbol{q}}_t)$ will be explained later. The controller $\boldsymbol{K}_{pos}$ is in charge of controlling the position and $\boldsymbol{K}_{att}$ is in charge of controlling the chaser attitude. They cope too with the attitude/position couplings in the chaser spacecraft. Couplings have several origins, e.g., flexible modes of the solar arrays and slosh phenomena (not considered in this thesis as already outlined), transverse inertia, relative orbital dynamics, capture mechanism offset with respect to the center of mass, etc..

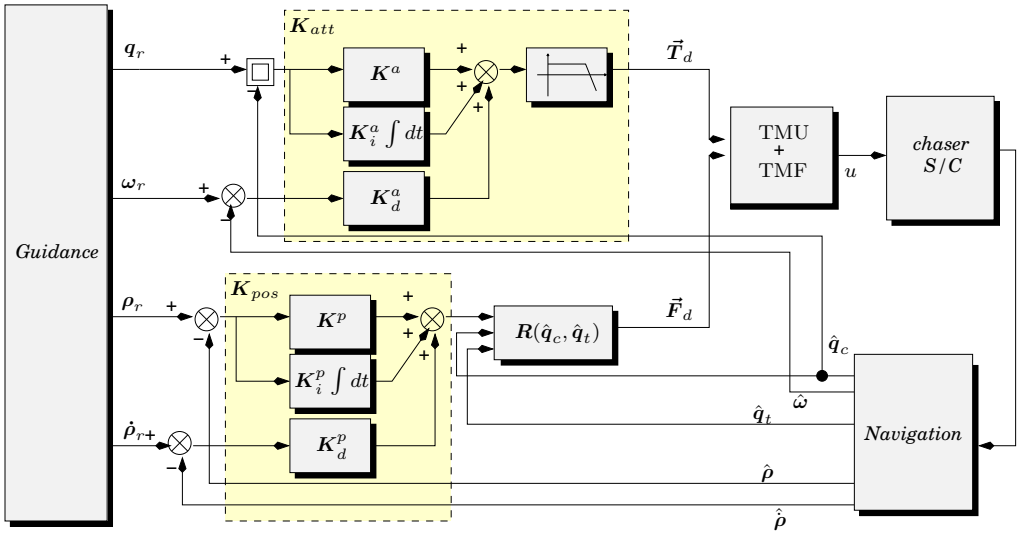


Figure 2.8 – GNC of the chaser spacecraft

2.2.3.1 Attitude Control Loop K_{att}

Suppose that the attitude of the chaser spacecraft is expressed in terms of the direction cosine matrix $\boldsymbol{A}_c$ relative to the reference frame in which the attitude manoeuvre is to be commanded and achieved (see Appendix A.4 for details on cosine direction matrix issues). Suppose that an attitude vector $\bar{\boldsymbol{\Theta}}$ has the components $\bar{\varphi}, \bar{\theta}, \bar{\psi}$ in a given frame and that the chaser is to be manoeuvred so that its final direction cosine matrix will coincide with a known matrix $\boldsymbol{A}_r$. In the following, this matrix is called the *reference matrix* and will refer to the frame in which $\boldsymbol{A}_r$ is defined. From a practical point of view, $\boldsymbol{A}_r$ is computed by the attitude guidance law.

According to the developments presented in Appendix A.4, the vector $\bar{\boldsymbol{\Theta}}$ can be expressed in the chaser frame and in the reference frame as $\boldsymbol{\Theta}_c$ and $\boldsymbol{\Theta}_r$ (respectively) in the following way:

$$\boldsymbol{\Theta}_c = \boldsymbol{A}_c \bar{\boldsymbol{\Theta}} \tag{2.15}$$

$$\boldsymbol{\Theta}_r = \boldsymbol{A}_r \bar{\boldsymbol{\Theta}} \tag{2.16}$$

Combining both equations, it yields

$$\boldsymbol{\Theta}_c = \boldsymbol{A}_c \boldsymbol{A}_r^{-1} \boldsymbol{\Theta}_r = \boldsymbol{A}_c \boldsymbol{A}_r^T \boldsymbol{\Theta}_r = \boldsymbol{A}_\epsilon \boldsymbol{\Theta}_r \tag{2.17}$$

The matrix $\boldsymbol{A}_\epsilon$, as defined in (2.17), has the following meaning: if the components of two non-collinear vectors $\boldsymbol{\Theta}_i$ are identical in both the chaser frame and the reference frame, then these frames coincide and the chaser body axes have reached the desired attitude in space. Hence, $\boldsymbol{A}_\epsilon$ is the direction cosine error matrix. When this matrix becomes an identity matrix, then $\boldsymbol{A}_c = \boldsymbol{A}_r$ and the chaser has reached the desired attitude. To clarify the meaning of this statement, the

matrix multiplication (2.17) is expanded as follows:

$$\boldsymbol{A}_\epsilon = \begin{bmatrix} a_{11c} & a_{12c} & a_{13c} \\ a_{21c} & a_{22c} & a_{23c} \\ a_{31c} & a_{32c} & a_{33c} \end{bmatrix} \begin{bmatrix} a_{11r} & a_{12r} & a_{13r} \\ a_{21r} & a_{22r} & a_{23r} \\ a_{31r} & a_{32r} & a_{33r} \end{bmatrix} = \begin{bmatrix} a_{11\epsilon} & a_{12\epsilon} & a_{13\epsilon} \\ a_{21\epsilon} & a_{22\epsilon} & a_{23\epsilon} \\ a_{31\epsilon} & a_{32\epsilon} & a_{33\epsilon} \end{bmatrix} \tag{2.18}$$

For the last matrix to become diagonal, the off-diagonal elements must be zeroed and the diagonal elements must become unit.

To understand the meaning of zeroing the off-diagonal elements, let examine Fig. 2.9 and interpret correctly the meaning of the elements $a_{ij\epsilon}$ in (2.18). For example, $a_{12\epsilon}$ is the scalar dot product between the $\vec{\boldsymbol{X}}_c$ and the $\vec{\boldsymbol{Y}}_r$ axes. Hence, $a_{12\epsilon} = 0$ is equivalent to making the $\vec{\boldsymbol{X}}_c$ axis perpendicular to the $\vec{\boldsymbol{Y}}_r$ axis by increasing the angle α in Fig. 2.9. This may be achieved by rotating the spacecraft about the $\vec{\boldsymbol{Z}}_c$ axis until the following equality is satisfied:

$$a_{12\epsilon} = \vec{\boldsymbol{X}}_c.\vec{\boldsymbol{Y}}_r = 0 \tag{2.19}$$

In the same way, it is easily seen that zeroing $a_{13\epsilon}$ is equivalent to the scalar dot product

$$a_{13\epsilon} = \vec{\boldsymbol{X}}_c.\vec{\boldsymbol{Z}}_r = 0 \tag{2.20}$$

which means geometrically that the spacecraft is to be rotated about its $\vec{\boldsymbol{Y}}_c$ axis until the $\vec{\boldsymbol{X}}_c$ axis becomes perpendicular to the $\vec{\boldsymbol{Z}}_r$ reference axis. Finally, rotation of about the $\vec{\boldsymbol{X}}_c$ axis will make the $\vec{\boldsymbol{Y}}_c$ axis perpendicular to the $\vec{\boldsymbol{Z}}_r$ axis, thus zeroing $a_{23\epsilon}$

$$a_{23\epsilon} = \vec{\boldsymbol{Y}}_c.\vec{\boldsymbol{Z}}_r = 0 \tag{2.21}$$

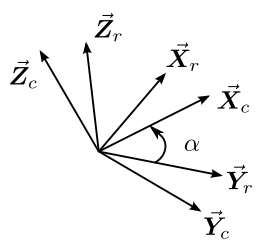


Figure 2.9 – Geometrical interpretation of zeroing the off-diagonal elements of A_ϵ.

By similar reasoning, it can be shown, that if both the reference and the chaser axis frames coincide, then the elements of the error matrix $\boldsymbol{A}_\epsilon$, that lie below the matrix diagonal are also zeroed. Thus, with the completion of the manoeuvre, the error matrix becomes the unit diagonal matrix. Simultaneous satisfaction of (2.19), (2.20) and (2.21) tends to rotate the chaser axis frame, so that it coincides with the desired target axis frame, thus achieving the desired attitude manoeuvre in space. Since the basic attitude dynamics of any spacecraft consists of two integrations per axis (see the modelling Section 2.4 addressed later), rate terms, i.e., $\boldsymbol{\omega} = [p\ q\ r]^T$, must be used in order to stabilize the spacecraft orientation along the three axes, leading to the following attitude control law:

$$T_{dx} = K_x^a a_{23\epsilon} + K_{xd}^a p_\epsilon \tag{2.22}$$

$$T_{dy} = K_y^a a_{13\epsilon} + K_{yd}^a q_\epsilon \tag{2.23}$$

$$T_{dz} = K_z^a a_{12\epsilon} + K_{zd}^a r_\epsilon \tag{2.24}$$

The terms $p_\epsilon, q_\epsilon, r_\epsilon$ are also used for damping purposes, the index ϵ being used to refer to errors (difference between desired and measured angular velocities, in the chaser frame).

In the beginning of a manoeuvre, the error elements may be quite large, depending on the initial relative attitude orientation of the chaser with respect to the reference frame. At the final stages of the attitude manoeuvre, when the axes are closely aligned with the reference frame axes, the error elements $a_{12\epsilon}$, $a_{13\epsilon}$ and $a_{23\epsilon}$ approach the errors of the Euler angles φ, θ, ψ. The control gains $K_x^a, K_y^a, K_z^a, K_{xd}^a, K_{yd}^a$ and K_{zd}^a should be designed so that, at the end of the large manoeuvre in space, the time responses will be well behaved. Also, sufficient stability margins in the frequency domain must be procured. These gains mainly depend on the inertia matrix.

There exists an equivalent quaternion error vector that can be associated to the cosine direction error matrix $\boldsymbol{A}_\epsilon$, see Appendix A.5 for quaternion definition and algebra.

As explained above, when dealing with direction cosine matrices, two consecutive attitude transformations are achieved by matrix multiplication of the two individual rotations, see (2.17). These two rotations can be expressed in the quaternion terminology by $\boldsymbol{A}(\boldsymbol{q}_r)$ for the first rotation and by $\boldsymbol{A}(\boldsymbol{q}_c)$ for the second one. The following expression holds for the overall attitude transformation in terms of direction cosine matrices

$$\boldsymbol{A}(\boldsymbol{q}_\epsilon) = \boldsymbol{A}(\boldsymbol{q}_r)\boldsymbol{A}(\boldsymbol{q}_c)^{-1} = \boldsymbol{A}(\boldsymbol{q}_r)\boldsymbol{A}(\boldsymbol{q}_c^{-1}) \tag{2.25}$$

In terms of quaternion notation, this equation leads to

$$\boldsymbol{q}_c^{-1}\boldsymbol{q}_r = \begin{bmatrix} q_{r0} & q_{r3} & -q_{r2} & q_{r1} \\ -q_{r3} & q_{r0} & q_{r1} & q_{r2} \\ q_{r2} & -q_{r1} & q_{r0} & q_{r3} \\ -q_{r1} & -q_{r2} & -q_{r3} & q_{r0} \end{bmatrix} \begin{bmatrix} -q_{c1} \\ -q_{c2} \\ -q_{c3} \\ q_{c0} \end{bmatrix} = \boldsymbol{q}_\epsilon \tag{2.26}$$

where $\boldsymbol{q}_\epsilon$, $\boldsymbol{q}_r$ and $\boldsymbol{q}_c$ are the error, reference and chaser quaternions, respectively. Since there is a one-to-one equivalence between the direction cosine matrix elements and the elements of the quaternion vector, i.e., a given direction cosine matrix $\boldsymbol{A} = [a_{ij}],\ i, j = 1, 2, 3$ and a quaternion $\boldsymbol{q} = (q_0, q_1, q_2, q_3)$

$$q_0 = \pm\frac{\sqrt{1 + a_{11} + a_{22} + a_{33}}}{2} \tag{2.27}$$

$$q_1 = \frac{a_{23} - a_{32}}{4q_0} \tag{2.28}$$

$$q_2 = \frac{a_{31} - a_{13}}{4q_0} \tag{2.29}$$

$$q_3 = \frac{a_{12} - a_{21}}{4q_0} \tag{2.30}$$

then equations (2.22)-(2.24) lead to the following attitude control law

$$T_{dx} = 2K_x^a q_{1\epsilon} q_{0\epsilon} + K_{xd}^a p_\epsilon \tag{2.31}$$

$$T_{dy} = 2K_y^a q_{2\epsilon} q_{0\epsilon} + K_{yd}^a q_\epsilon \tag{2.32}$$

$$T_{dz} = 2K_z^a q_{3\epsilon} q_{0\epsilon} + K_{zd}^a r_\epsilon \tag{2.33}$$

Performing the computation of $\boldsymbol{q}_\epsilon$ in (2.26) requires fewer algebraic operations than computing

the elements in $\boldsymbol{A}_\epsilon$. This is one reason why the control law of (2.31)-(2.33) is preferred to that of (2.22)-(2.24) in the case of the MSR mission, although they are equivalent from a physical point of view.

Finally, since the advantages of an integral part in control laws are well known, the attitude control law $\boldsymbol{K}_{att}$ of the chaser is given by

$$T_{dx} = 2K_x^a q_{1\epsilon} q_{0\epsilon} + 2K_{xi}^a \int q_{1\epsilon} q_{0\epsilon} dt + K_{xd}^a p_\epsilon \tag{2.34}$$

$$T_{dy} = 2K_y^a q_{2\epsilon} q_{0\epsilon} + 2K_{yi}^a \int q_{2\epsilon} q_{0\epsilon} dt + K_{yd}^a q_\epsilon \tag{2.35}$$

$$T_{dz} = 2K_z^a q_{3\epsilon} q_{0\epsilon} + 2K_{zi}^a \int q_{3\epsilon} q_{0\epsilon} dt + K_{zd}^a r_\epsilon \tag{2.36}$$

where the gains $K_{xi}^a, K_{yi}^a, K_{zi}^a$ are designed to manage the dynamics of disturbances rejection.

Finally and as it can be noted on Fig. 2.8, the control law (2.34)-(2.36) is followed by a low pass filter which is also useful in order to prevent high frequency behaviour of the controller outputs $T_d = [T_{dx}\ T_{dy}\ T_{dz}]^T$.

Remark 2.3. *Note, that usually another role of this filter is to reject the flexible modes of the solar arrays. However, since the solar arrays modes are not implemented in the MSR simulator provided by Thales Alenia Space, this aspect is not considered in this thesis.*

Remark 2.4. *The directional cosines based formulation of* (2.31)-(2.33) *is given by*

$$T_{dx} = -\frac{1}{2} K_x^a (a_{32\epsilon} - a_{23\epsilon}) + K_{xd}^a p_\epsilon \tag{2.37}$$

$$T_{dy} = -\frac{1}{2} K_y^a (a_{13\epsilon} - a_{31\epsilon}) + K_{yd}^a q_\epsilon \tag{2.38}$$

$$T_{dz} = -\frac{1}{2} K_z^a (a_{21\epsilon} - a_{12\epsilon}) + K_{zd}^a r_\epsilon \tag{2.39}$$

When small angles are considered, the terms $a_{ij\epsilon}$ can be linearly approximated and the control law behaves as a classical linear controller (PD controller in this case or PID when considering an integral part). This approximation is useful, since it enables to analyse the degree of stability of the control law by computing the minimum gain margin, phase margin and associated crossover frequencies over each axis X, Y, Z considering that the other axes are in closed loop. This is usually the practical analysis done in space industries, even if it is more relevant to consider the controller in its MIMO form.

2.2.3.2 Position Control Loop $\boldsymbol{K}_{pos}$

The design of the chaser position control law $\boldsymbol{K}_{pos}$ obeys to the classical theory of the PID controllers. Consider the theoretical developments given in Section 2.4.1 that addresses the modelling of the relative motion of the chaser with respect to the target spacecraft. As it is shown, under the assumption of a rendezvous on a circular orbit, the nonlinear equations

governing the dynamics of the chaser are given in the local frame according to

$$\ddot{\xi}(t) = 3n^2\xi(t) + 2n\dot{\eta}(t) + F_{t\xi}(t) + F_{p\xi}(t) \tag{2.40}$$
$$\ddot{\eta}(t) = -2n\dot{\xi}(t) + F_{t\eta}(t) + F_{p\eta}(t) \tag{2.41}$$
$$\ddot{\zeta}(t) = -n^2\zeta(t) + F_{t\zeta}(t) + F_{p\zeta}(t) \tag{2.42}$$

where the X-axis is along the radius vector of the target spacecraft, the Z-axis is along the angular momentum vector of the target spacecraft, and the Y-axis completes the right handed system. With this definition, the central body is towards the negative X direction and the Y-axis points along the velocity vector of the target spacecraft, see Fig. 2.5 for an illustration. $\boldsymbol{F}_t = [F_{t\xi}\ F_{t\eta}\ F_{t\zeta}]^T$ is the control input vector that is due to the thruster-based propulsion unit and $\boldsymbol{F}_p = [F_{p\xi}\ F_{p\eta}\ F_{p\zeta}]^T$ is a generalized disturbance vector, both given in the local frame. The definition of $\boldsymbol{F}_p$ is considered later, since it is not of prime interest here.

Since equations (2.40)-(2.42) define a linear state-space model, it is natural to think about linear methods from the robust control community to design the position control law. This leads to the definition of the control structure as depicted on Fig. 2.8, i.e., the position control law consists of two successive functions:

- a linear controller that is designed on the model given by equations (2.40)-(2.42) and that generates $\boldsymbol{F}_t$, and

- a rotation matrix that is in charge to transform the outputs $\boldsymbol{F}_t$ of the linear controller $\boldsymbol{K}_{pos}(s)$ into the chaser frame, i.e

$$\boldsymbol{F}_d = \boldsymbol{R}(\hat{\boldsymbol{q}}_c, \hat{\boldsymbol{q}}_t)\boldsymbol{F}_t \tag{2.43}$$

  $\hat{\boldsymbol{q}}_c$ and $\hat{\boldsymbol{q}}_t$ also denote the quaternion of the chaser and the target respectively. The notation "$\hat{\bullet}$" indicates that these quaternions are estimated by the navigation unit.

So the major concern is the design of the linear controller $\boldsymbol{K}_{pos}(s)$.

One solution that is well mastered by the space industries obeys to the so-called "in-plane" and "out-of-plane" separation principle. Noting that (2.42) is autonomous, the system of (2.40) - (2.42) can be split into two independent systems of equations, i.e.,

$$\ddot{\xi}(t) = 3n^2\xi(t) + 2n\dot{\eta}(t) + F_{t\xi}(t) + F_{p\xi}(t) \tag{2.44}$$
$$\ddot{\eta}(t) = -2n\dot{\xi}(t) + F_{t\eta}(t) + F_{p\eta}(t) \tag{2.45}$$

and

$$\ddot{\zeta}(t) = -n^2\zeta(t) + F_{t\zeta}(t) + F_{p\zeta}(t) \tag{2.46}$$

Motions along X-axis and Y-axis are "in-plane" and are concerned by (2.44)-(2.45) and motion along the Z-axis is *out-of-plane* and is concerned by (2.46). Note, that motion along the Y-axis is referred as *along-track* due to the capture scenario.

Finally, considering that the term $2n\dot{\eta}$ can be neglected in (2.44), (2.44)-(2.46) become a simple

system of three SISO systems. A PID control law immediately follows such as

$$F_{t\xi} = K^p_\xi \xi_\epsilon + K^p_{\xi i} \int \xi_\epsilon dt + K^p_{\xi d} \dot{\xi}_\epsilon \tag{2.47}$$

$$F_{t\eta} = K^p_\eta \eta_\epsilon + K^p_{\eta i} \int \eta_\epsilon dt + K^p_{\eta d} \dot{\eta}_\epsilon \tag{2.48}$$

$$F_{t\zeta} = K^p_\zeta \zeta_\epsilon + K^p_{\zeta i} \int \zeta_\epsilon dt + K^p_{\zeta d} \dot{\zeta}_\epsilon \tag{2.49}$$

The parameters $K^p_\xi, K^p_\eta, K^p_\zeta, K^p_{\xi i}, K^p_{\eta i}, K^p_{\zeta i}, K^p_{\xi d}, K^p_{\eta d}$ and $K^p_{\zeta d}$ are designed to ensure some control objectives, e.g., to ensure the required capture performance requirements. Signals $\xi_\epsilon = \xi_r - \hat{\xi}$, $\eta_\epsilon = \eta_r - \hat{\eta}$, $\zeta_\epsilon = \zeta_r - \hat{\zeta}$, $\dot{\xi}_\epsilon = \dot{\xi}_r - \hat{\dot{\xi}}$, $\dot{\eta}_\epsilon = \dot{\eta}_r - \hat{\dot{\eta}}$, and $\dot{\zeta}_\epsilon = \dot{\zeta}_r - \hat{\dot{\zeta}}$ refer to the position and velocity errors. Signals $\boldsymbol{\rho}_r = [\xi_r \ \eta_r \ \zeta_r]^T$, $\dot{\boldsymbol{\rho}}_r = [\dot{\xi}_r \ \dot{\eta}_r \ \dot{\zeta}_r]^T$ and $\hat{\boldsymbol{\rho}} = [\hat{\xi} \ \hat{\eta} \ \hat{\zeta}]^T$, $\hat{\dot{\boldsymbol{\rho}}} = [\hat{\dot{\xi}} \ \hat{\dot{\eta}} \ \hat{\dot{\zeta}}]^T$ are provided by the guidance and navigation units respectively.

2.2.3.3 Robustness Margins and Performances

The stability and performance of the resulting controllers are illustrated on Fig. 2.10 and 2.11 which plot the open-loop transfers on each axis considering, that the other axes are in closed loop. Figure 2.10 is concerned by the attitude control and Fig. 2.11 is concerned by the position control. Zooms are presented for a better illustration of the robustness margins and performances. A scattering of the uncertainties is performed following the numerical values reported in Table 2.3. The red large curve corresponds to the nominal cases.

Property	Nominal value	Unit	Uncertainty	Distribution
Mass (m_c)	1575	kg	±10%	$\mathcal{N}(1, 0.1/3)$
Inertia matrix ($\boldsymbol{J}$)	$\begin{bmatrix} 1450 & -20 & 5 \\ -20 & 1800 & -5 \\ 5 & -5 & 1200 \end{bmatrix}$	$\text{kg} \cdot \text{m}^2$	±20%	$\mathcal{N}(1, 0.2/3)$
CoM ($\boldsymbol{d}_{CoM}$)	$\begin{bmatrix} 0.880 & 0.035 & 0.035 \end{bmatrix}^T$	m	±3cm	$\mathcal{N}(0, 0.03/3)$
Thrust ($\lVert F_T \rVert$)	$22 \times (N$-thrusters)	N	±1%	$\mathcal{N}(1, 0.01)$
Cartesian coordinates ($\boldsymbol{x}_p$)	Converted orbital elements, see Table 2.2	m, m/s	±10%	$\mathcal{N}(1, 0.1/3)$
MIB	0.068	s	n/a	n/a
ON-time quantisation step	0.01	s	n/a	n/a

Table 2.3 – Considered parameter uncertainties of the chaser spacecraft

Each color in the plot (magenta, red and blue for the X ,Y and Z-axes, respectively) corresponds to a stack of the same SISO transfer obtained with different numerical values of the plant parameters. These plots show that the obtained range of the phase margin P_m, of the gain margin G_m, and the bandwidth ω_u are given according to

- Attitude: $G_m \approx [-14.5 \text{ dB} \ ; 14.5 \text{ dB}]$, $P_m \approx [49^o \ ; 58^o]$, $\omega_u \approx 0.1$ rad/s

- Position: $G_m \approx [-15 \text{ dB} \ ; -10.6 \text{ dB}]$, $P_m \approx [54^o \ ; 68^o]$, $\omega_u \approx 0.1$ rad/s

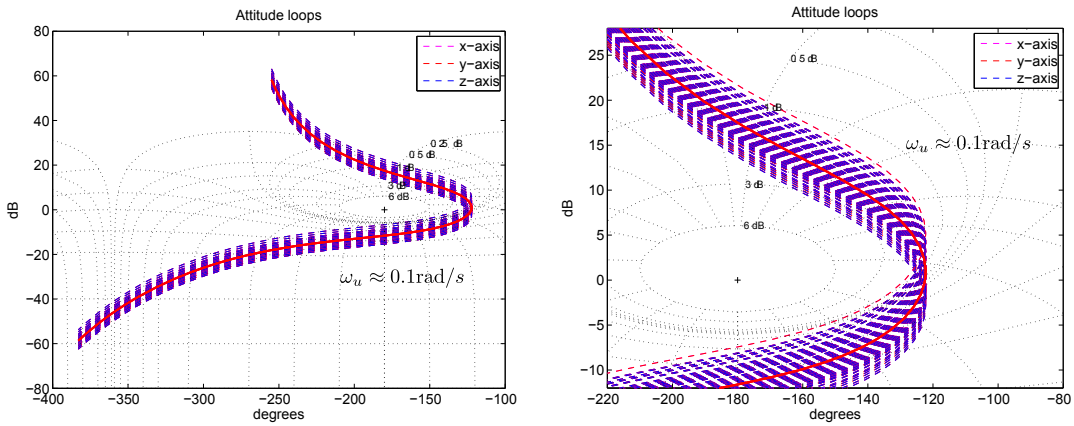


Figure 2.10 – Robustness margins and performances of the attitude control loop

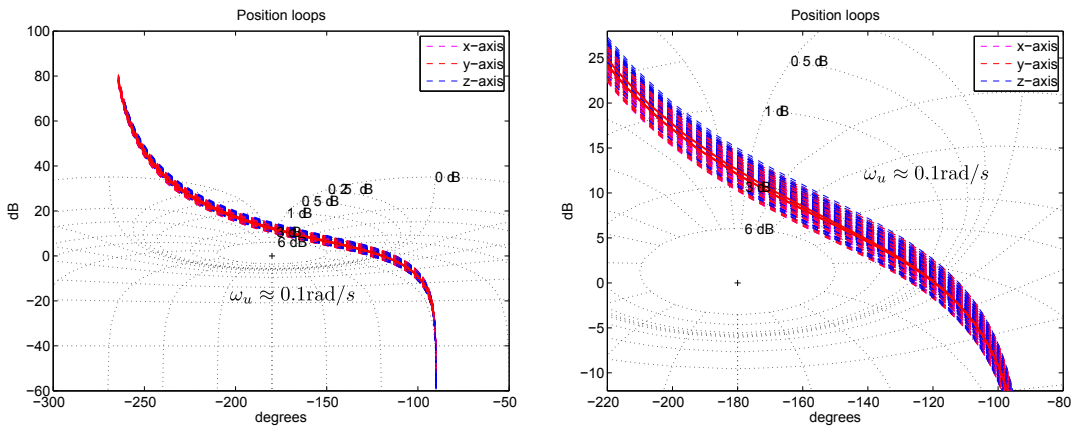


Figure 2.11 – Robustness margins and performances of the position control loop

2.2.3.4 Actuator Management Functions

The controller outputs, the desired force $\boldsymbol{F}_d$ and the desired torque $\boldsymbol{T}_d$, (see Fig. 2.8) are next sent to the Thruster Modulator Unit (TMU), that integrates the small commanded pulses which are below the Minimum Impulse Bit (MIB) and releases a pulse ($\boldsymbol{F}_{\tilde{d}}$ or/and $\boldsymbol{T}_{\tilde{d}}$) when the total reaches a momentum threshold. The MIB shall not be too large as this corresponds to a delay from the controller viewpoint. The TMU is widely used to compensate actuator nonlinearities and to increase control accuracy [238, 239]. The purpose of on-board Thruster Management Function (TMF) is to select specific thrusters at each control cycle and to compute their scaled firing times $\tilde{u}_i$ to realize force $\boldsymbol{F}_{\tilde{d}}$ and torque $\boldsymbol{T}_{\tilde{d}}$ command impulses coming from the TMU.

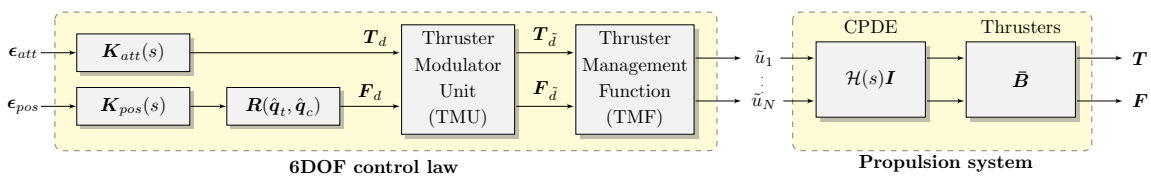


Figure 2.12 – Control law (left) and the propulsion system (right) of the chaser vehicle

Note, that the TMF is nothing else than an online control allocation algorithm, see Section 1.4.3 which addresses the state of the art of CA methods[1]. The baseline TMF algorithm relies on a simplified approach with respect to the Simplex and thruster non-linearities (minimum On/Off times) [239]. The chaser control law and propulsion system are summarised in Fig. 2.12.

Regarding the propulsion system, all thrusters have fixed direction $\boldsymbol{d}_i \in \mathbb{R}^3, i \in \mathcal{S}_{all}$. The set $\mathcal{S}_{all} = \{1, 2, \ldots N\}$ denotes the set of all thruster indices. Each thruster is able to produce a maximum thrust of $||F_T|| = 22$ N. The Chemical Propulsion Drive Electronics (CPDE), that drives the thrusting actuators, initiates the opening of the thruster valves for the commanded durations $0 \leq \tilde{u}_i \leq 1, \forall i \in \mathcal{S}_{all}$. Variables $\tilde{u}_i$ are in fact scaled ON times (firing intervals). The scaling is done versus the sampling period T of the control unit and is defined according to $\tilde{u}_i(t_k) = T_{on_i}(t_k)/T$, where $T_{on_i}(t_k)$ is the actual/real firing duration (ON time) of the ith thruster at control cycle $t_k = kT$, see Fig. 2.13 for an illustration.

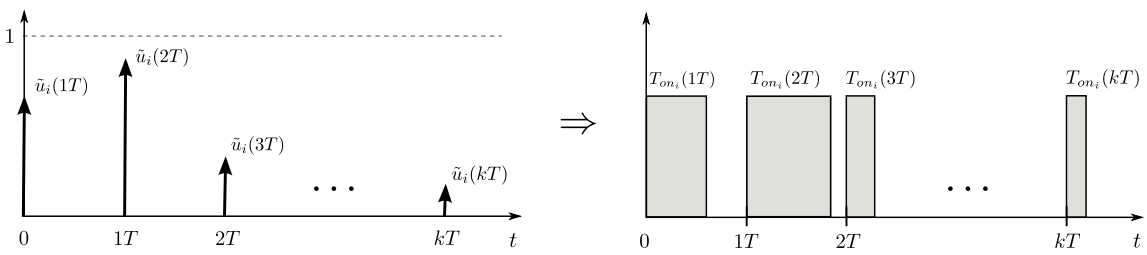


Figure 2.13 – Scaled ON-times versus real thruster firing durations

The propulsion system is obviously a source of uncertainty in the system. The linear parameter-varying transfer function

$$\mathcal{H}(s) = e^{-\tau(t)s} \tag{2.50}$$

aims to model the effect of the unknown time-varying delays induced by the CPDE electronic device and the uncertainties on the thruster rise times [110, 237]. The delay $\tau(t)$ is assumed to be unknown and time-varying, but upper bounded by a known constant $\bar{\tau}$, i.e., $\tau(t) \leq \bar{\tau}$. Furthermore, it is assumed that each thruster is delayed with the same delay $\tau(t)$. This is a reasonable assumption from the practical point of view, since for all nominal thrusters, the same CPDE device is used to control the openings of the thruster valves.

To proceed, let $\tilde{u}_k(t - \tau(t))$ be the commanded open duration of the kth thruster delayed by $\tau(t)$, then the net forces and torques generated by the thrusters (in fault free case) are given in the chaser body fixed frame according to (see Fig. 2.12)

$$\boldsymbol{F}(t) = \boldsymbol{B}_F \tilde{\boldsymbol{u}}(t - \tau(t)), \quad \boldsymbol{T}(t) = \boldsymbol{B}_T \tilde{\boldsymbol{u}}(t - \tau(t)) \tag{2.51}$$

In this equation $\tilde{\boldsymbol{u}}(t) = [\tilde{u}_1(t), \tilde{u}_2(t), \ldots, \tilde{u}_N(t)]^T$, and

$$\boldsymbol{B}_F = \left[\boldsymbol{b}_{F_1}, \boldsymbol{b}_{F_2}, \ldots, \boldsymbol{b}_{F_N}\right], \quad \boldsymbol{B}_T = \left[\boldsymbol{b}_{T_1}, \boldsymbol{b}_{T_2}, \ldots, \boldsymbol{b}_{T_N}\right] \tag{2.52}$$

are the thruster sensitivity (configuration) matrices with[2]

$$\boldsymbol{b}_{Fk} = -\boldsymbol{d}_k ||F_T||, \quad \boldsymbol{b}_{Tk} = (\boldsymbol{d}_{p_k} - \boldsymbol{d}_{CoM}) \times \boldsymbol{b}_{Fk}, \quad \forall k \in \mathcal{S}_{all}$$

[1]The "TMF" is a more general term linked with control allocation and used within an industrial context.

[2]Due to confidential reasons, the numerical values with regards to the spacecraft geometry and characteristics are omitted.

where " $\times$ " denotes the cross product of vectors, $\boldsymbol{d}_{CoM} \in \mathbb{R}^3$ is the position vector of the CoM from the chaser geometrical center, and $\boldsymbol{d}_{p_k} \in \mathbb{R}^3, \forall k \in \mathcal{S}_{all}$ are the position (location) vectors of the thrusters. The overall, 6 DOF, thruster configuration matrix $\bar{\boldsymbol{B}}$ is defined by

$$\bar{\boldsymbol{B}} = \begin{bmatrix} \boldsymbol{B}_T \\ \boldsymbol{B}_F \end{bmatrix} \in \mathbb{R}^{6\times N} \tag{2.53}$$

The columns of $\boldsymbol{B}_F$ and $\boldsymbol{B}_T$ are the influence coefficients defining how each thruster affects each component of $\boldsymbol{F}$ and $\boldsymbol{T}$, respectively.

2.3 Failure Management and Fault Considerations

The GNC unit described in the previous sections is also an important system to carry out the success of the rendezvous and to guarantee the necessary performance for the capture. However, it is clear that to prevent a mission avoidance, the chaser has to be equipped by a failure detection and recovery management unit, able to cover any failures in its different systems and subsystems.

Common fault diagnosis and accommodation architectures used by space industries, rely on a hierarchical implementation of failure detection and management. This is also the case of the chaser spacecraft [83, 239].

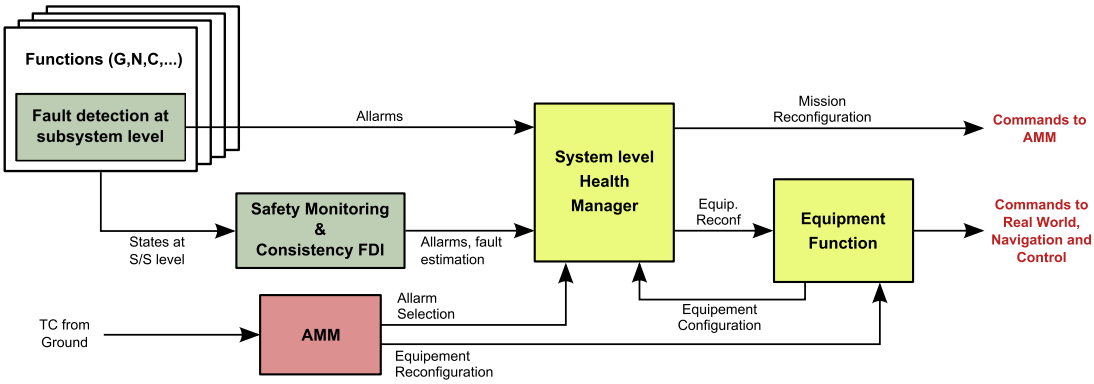


Figure 2.14 – Failure management unit with the location of the failure detection units

Recent study Peuvédic et al. [240] demonstrate that the failure management system tend to cover completely all the system and subsystem failures in the case of the MSR mission, consisting of two separate (main) functions, see Fig. 2.14 for an illustration. The Autonomous Mission Management (AMM) function is not considered here, since it is completely out of the scope of this study.

- The first failure detection set of functions, implemented at the GNC level (and more precisely at the navigation level) is in charge to detect faults at subsystem level. The main functions are:
  - the detection of sudden sensor death,
  - the detection of sudden frozen signals (lock-in-place fault type) coming from a sensor,
  - the consistency check between the two IMUs, and

  - the consistency check between IMUs in "hot redundancy" configuration and STRs in "cold redundancy" configuration. Hot and cold redundancy is a terminology used by space industries to outline, that all redundant sensors are switched on (hot) or only one of the redundant sensor is switched on, the others being switched off and waiting for a possible use (cold).

- The second failure detection set of functions, implemented at the Safety Monitoring level, is in charge of the detection of failures at actuator level or at higher level. The main functions of this set are:
  - checking the consistency between the tachometers and the commands sent to the reaction wheels (not used in this study as already mentioned),
  - checking the consistency between the IMUs and the commands sent to the thrusters,
  - checking the chaser trajectory with respect to predefined rendezvous corridors,
  - checking the approach velocity,
  - checking the trajectory of the chaser with respect to collision risks,
  - checking the convergence of the controller output signals during the whole rendezvous phase, and
  - finally, monitoring the power.

All these functions are hierarchized into five levels. These levels with the functions they are concerned by, are summarized in Table 2.4.

Levels	Interest
Level 1 sensor checks	Monitoring of the outputs of all the sensors. This level covers most of the sensor faults such as sudden sensor death and lock-in-place fault types.
Level 2 IMU/IMU	Interest is limited to the detection of failures not seen by level 1 (i.e., unlikely slow drifts of IMUs).
Level 2 IMU/STR	Interest is limited to the detection of failures not seen by level 1.
Level 3 thruster/IMU	Check is done during the whole rendezvous. The IMU hot redundancy enables to discard IMU failures in the thruster/IMU inconsistency, leading model-based techniques viable candidates.
Level 3 wheel/tachometer	This check covers most of wheels faults. The isolation is immediate since a tachometer is available on each wheel.
Level 4 approach corridors	Monitor the position/velocity of the chaser versus the approach corridors.
Level 4 collision risks	Detect if a collision may occur between the spacecraft.
Level 4 mode success	Detect the divergence of the controller outputs.
Level 5 power alarm	Protection against ground operation errors and electrical subsystem failures.

Table 2.4 – Hierarchical fault detection levels

Failure accommodation and recovery are managed by the System Health Management (SHM) unit, see Fig. 2.14. This unit manages the type of corrective actions to be applied

- at equipment level: switching to a redundant set of equipments, e.g., sensor in hot redundancy (IMU case), or propagation of last valid measurement during the switch-on of the redundant module in cold redundancy (STR case), switching to a redundant set of actuators, etc.,

- at GNC level: switching to a different guidance mode/sub-mode, or new control allocation, and

- at mission level: triggering a collision avoidance maneuver and transfer to a safe waiting orbit, or simple retreating.

In this thesis, model-based FDI solutions, that fit the above described fault management architecture are proposed. More precisely, Chapter 3 will address a FDIR solution that can be integrated in level 3 as it is, the recovery principle being exactly those used by the SHM, i.e., switching to a redundant set of equipments. Chapter 4 will address a more enhanced solution, since it relies on an active FTC approach. However, since an active FTC approach involves an FDI unit, it is guaranteed that the FDI part can be embedded at level 3. In other words, all solutions proposed in this thesis must be understood to be an integral part of the overall failure management unit currently developed by Thales Alenia Space for the MSR mission.

2.3.1 Description of the Set of Detection Functions at the Subsystem Level

The lowest fault detection function implemented as the subsystem level (level 1) is concerned by the sensors. It monitors directly their outputs. If a signal becomes null, while the sensor state is operational, an alarm "dead sensor" is raised.

To detect a lock-in-place fault type in the sensors, the technique is based on the comparison between the output of a sensor and its time derivative. Let $s_i(t)$ denote the output of the ith sensor, then $s_i(t) - \frac{ds_i(t)}{dt}$ defines a fault indicating signal for the lock-in-place fault type. Similarly to the "dead sensor" fault monitoring technique, the lock-in-place monitoring is activated if the sensor is operational. Furthermore, this monitoring is activated only if $s_i(t)$ is not null (i.e., dead sensor), providing a hierarchical approach between these two kinds of faults.

The higher monitoring level (level 2) is concerned by the IMU/IMU and the IMU/STR consistency checks. This monitoring is also activated if the IMUs and the STRs are operational and if a fault has not been detected at the previous level.

The IMU/IMU consistency check relies on the (static) parity space approach, see Chapter 1 if necessary. To proceed, let us denote $\mathcal{F}_{IMU1} = \{O_{IMU1}; \vec{X}_{IMU1}, \vec{Y}_{IMU1}, \vec{Z}_{IMU1}\}$ and $\mathcal{F}_{IMU2} = \{O_{IMU2}; \vec{X}_{IMU2}, \vec{Y}_{IMU2}, \vec{Z}_{IMU2}\}$ the frames in which the measurement signals of the first and second IMU are delivered, and consider the body frame $\mathcal{F}_b = \{O_B; \vec{\boldsymbol{X}}_b, \vec{\boldsymbol{Y}}_b, \vec{\boldsymbol{Z}}_b\}$ illustrated in Fig. 2.18 (the center of this frame is fixed to the center of mass of the chaser). Then, it

follows

$$\dot{\boldsymbol{\omega}}^{\mathcal{F}_b}(t) = \boldsymbol{R}_1 \dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU1}}(t) \tag{2.54}$$
$$\dot{\boldsymbol{\omega}}^{\mathcal{F}_b}(t) = \boldsymbol{R}_2 \dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU2}}(t) \tag{2.55}$$
$$\boldsymbol{\omega}^{\mathcal{F}_b}(t) = \boldsymbol{R}_1 \boldsymbol{\omega}^{\mathcal{F}_{IMU1}}(t) \tag{2.56}$$
$$\boldsymbol{\omega}^{\mathcal{F}_b}(t) = \boldsymbol{R}_2 \boldsymbol{\omega}^{\mathcal{F}_{IMU2}}(t) \tag{2.57}$$

where $\boldsymbol{R}_1 \in \mathbb{R}^3$ and $\boldsymbol{R}_2 \in \mathbb{R}^3$ are rotation matrices in charge of mapping the signals from $\mathcal{F}_{IMU1}$ and $\mathcal{F}_{IMU2}$ to $\mathcal{F}_b$[3]. These four relations allow to define the following residual vectors

$$\boldsymbol{r}_{\dot{\omega}1}(t) = \dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU1}}(t) - \boldsymbol{R}_1^{-1}\boldsymbol{R}_2 \dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU2}}(t), \quad \boldsymbol{r}_{\dot{\omega}1} \in \mathbb{R}^3 \tag{2.58}$$
$$\boldsymbol{r}_{\dot{\omega}2}(t) = \dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU2}}(t) - \boldsymbol{R}_2^{-1}\boldsymbol{R}_1 \dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU1}}(t), \quad \boldsymbol{r}_{\dot{\omega}2} \in \mathbb{R}^3 \tag{2.59}$$
$$\boldsymbol{r}_{\omega1}(t) = \boldsymbol{\omega}^{\mathcal{F}_{IMU1}}(t) - \boldsymbol{R}_1^{-1}\boldsymbol{R}_2 \boldsymbol{\omega}^{\mathcal{F}_{IMU2}}(t), \quad \boldsymbol{r}_{\omega1} \in \mathbb{R}^3 \tag{2.60}$$
$$\boldsymbol{r}_{\omega2}(t) = \boldsymbol{\omega}^{\mathcal{F}_{IMU2}}(t) - \boldsymbol{R}_2^{-1}\boldsymbol{R}_1 \boldsymbol{\omega}^{\mathcal{F}_{IMU1}}(t), \quad \boldsymbol{r}_{\omega2} \in \mathbb{R}^3 \tag{2.61}$$

For residual evaluation, the GLR test is applied to each component of the residual vectors, see Appendix B for some issues about the GLR test. The decision making is done through a threshold based approach, i.e., if the GLR test is higher that a given threshold, then a Boolean is set. Because in a given frame, accelerometers (providing $\dot{\boldsymbol{\omega}} = [\dot{p}\ \dot{q}\ \dot{r}]^T$) and gyroscopes (providing $\boldsymbol{\omega} = [p\ q\ r]^T$) can be diagnosed axis per axis and IMU per IMU, it leads to the isolation of the faulty axis to be immediate.

A special case is concerned by the case of simultaneous drifts on the three axes of a given IMU, say the accelerometer to illustrate the technique. In such a case, because the fault manifests itself on all components of $\boldsymbol{r}_{\dot{\omega}1}$ and $\boldsymbol{r}_{\dot{\omega}2}$, it is necessary to have a dedicated signal-based technique to identify which accelerometer (IMU) is faulty. The basic of the principle is to look for the maximum covariance of the augmented residual vector $[\boldsymbol{r}_{\dot{\omega}1}^T\ \boldsymbol{r}_{\dot{\omega}2}^T]^T$ and the measurements $\dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU1}}$ and $\dot{\boldsymbol{\omega}}^{\mathcal{F}_{IMU2}}$ separately. Those that admits the maximum covariance is retained to be faulty. Figure 2.15 (left) illustrates a sensor drift in the 1st accelerometer on all the 3 axes simultaneously. This corresponds to the most difficult fault to be diagnosed since, in this case, both the residuals are affected. Thus, in order to make a final decision about the faulty IMU, the maximum covariance principle explained above is used. Figure 2.15 (right) considers a performance degradation (increased noise) in the z-axis of the second gyro. In this case, the GLR test plays an important role to identify which axis is faulty.

Similarly to the fault monitoring technique explained above, the IMU/STR consistency check is activated if no fault is declared by the IMU/IMU consistency check. The IMU/STR consistency check relies on a H_∞ observer based on the relation between the rotational velocities $\boldsymbol{\omega}$ and the rate of the Euler angles $\dot{\boldsymbol{\Theta}} = [\dot{\varphi}\ \dot{\theta}\ \dot{\psi}]^T$, in the body frame $\mathcal{F}_b$. Its inverse relationship describes the kinematic equations for the attitude [296]. For clarity, the notation superscript $\mathcal{F}_b$ is omitted in the following developments.

$$\dot{\boldsymbol{\Theta}}(t) = \boldsymbol{h}(\boldsymbol{\Theta}(t))\boldsymbol{\omega}(t) = \frac{1}{\cos(\theta)} \begin{bmatrix} \cos(\theta) & \sin(\varphi)\sin(\theta) & \cos(\varphi)\sin(\theta) \\ 0 & \cos(\varphi)\cos(\theta) & -\sin(\varphi)\cos(\theta) \\ 0 & \sin(\varphi) & \cos(\varphi) \end{bmatrix} \boldsymbol{\omega}(t) \tag{2.62}$$

Since the IMUs and the STR deliver the measure of $\boldsymbol{\omega}$ and $\boldsymbol{\Theta}$, this equation suggests the following

[3]The numerical values of $\boldsymbol{R}_1$ and $\boldsymbol{R}_2$ are not given there due to confidential reasons.

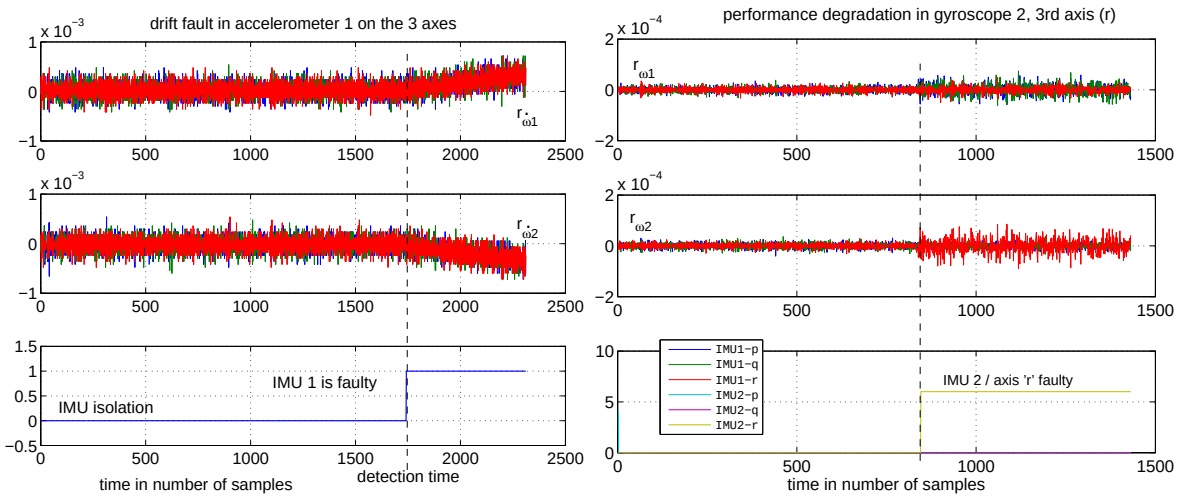


Figure 2.15 – Sensor drift in the 1st accelerometer (left) and performance degradation of the 2nd gyro (right)

observer–based fault detector for STR faults:

$$\begin{cases} \dot{\hat{\boldsymbol{\Theta}}}(t) = \boldsymbol{h}(\hat{\boldsymbol{\Theta}}(t))\boldsymbol{\omega}(t) + \boldsymbol{L}(\boldsymbol{y}(t) - \hat{\boldsymbol{y}}(t)) \\ \hat{\boldsymbol{y}}(t) = \hat{\boldsymbol{\Theta}}(t) \\ \boldsymbol{r}_\Theta(t) = \boldsymbol{y}(t) - \hat{\boldsymbol{y}}(t), \quad \boldsymbol{r}_\Theta \in \mathbb{R}^3 \end{cases} \tag{2.63}$$

The problem then turns out to be the design of the matrix gain $\boldsymbol{L}$. Here, a linear approximation of (2.62) is used so that equation (2.63) becomes a linear observer in a form that is suitable for the design of the gain $\boldsymbol{L}$ using H_∞ techniques.

To proceed, consider equation (2.62) linearly approximated around $\boldsymbol{\Theta} = \boldsymbol{0}$. From a practical point of view, since there exists noises and misalignment errors in the sensors, it can be verified that (2.62) can be written according to

$$\begin{cases} \dot{\boldsymbol{\Theta}}(t) = \boldsymbol{A}_\Theta \boldsymbol{\Theta}(t) + \boldsymbol{B}_\Theta \boldsymbol{\omega}(t) + \boldsymbol{\Gamma}\boldsymbol{w}(t) \\ \boldsymbol{y}(t) = \boldsymbol{\Theta}(t) + \boldsymbol{v}(t) \end{cases} \tag{2.64}$$

The state noise $\boldsymbol{w}$ distributed by $\boldsymbol{\Gamma}$ aims at modelling the errors due to the linearization and the IMUs misalignments and noises, whereas the measurement noise $\boldsymbol{v}$ aims at modelling STRs misalignment errors and noises.

The H_∞ techniques consider that the state and measurement noises $\boldsymbol{w}$ and $\boldsymbol{v}$ have frequency spectrum which can be approximated by linear dynamics with normalized inputs $\boldsymbol{d}_i$, i.e.,

$$\begin{cases} \dot{\boldsymbol{x}}_w(t) = \boldsymbol{A}_w \boldsymbol{x}_w(t) + \boldsymbol{B}_w \boldsymbol{d}_1(t) \\ \boldsymbol{w}(t) = \boldsymbol{C}_w \boldsymbol{x}_w(t) + \boldsymbol{D}_w \boldsymbol{d}_1(t) \end{cases}, \quad \begin{cases} \dot{\boldsymbol{x}}_v(t) = \boldsymbol{A}_v \boldsymbol{x}_v(t) + \boldsymbol{B}_v \boldsymbol{d}_2(t) \\ \boldsymbol{v}(t) = \boldsymbol{C}_v \boldsymbol{x}_v(t) + \boldsymbol{D}_v \boldsymbol{d}_3(t) \end{cases} \tag{2.65}$$

where $\boldsymbol{d}_i, i = 1, 2, 3$ are assumed to be of arbitrary spectrum with unit 2-norm. Since $\boldsymbol{d}_2$ acts like a state noise through the shaping filter dynamics, a separate noise, $\boldsymbol{d}_3$, is used in the feed-forward term of the model of $\boldsymbol{v}$ to prevent the state and measurement noise from being correlated. With these shaping filters, the design problem can be formulated within the H_∞ setting according to

the following equations with the normalized input $\boldsymbol{d} = [\boldsymbol{d}_1^T \ \boldsymbol{d}_2^T \ \boldsymbol{d}_3^T]^T$:

$$\begin{bmatrix} \dot{\boldsymbol{\Theta}}(t) \\ \dot{\boldsymbol{x}}_w(t) \\ \dot{\boldsymbol{x}}_v(t) \end{bmatrix} = \begin{bmatrix} \boldsymbol{A}_\Theta & \boldsymbol{\Gamma}\boldsymbol{C}_w & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{A}_w & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{A}_v \end{bmatrix} \begin{bmatrix} \boldsymbol{\Theta}(t) \\ \boldsymbol{x}_w(t) \\ \boldsymbol{x}_v(t) \end{bmatrix} + \begin{bmatrix} \boldsymbol{\Gamma}\boldsymbol{D}_w & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{B}_w & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{B}_v & \boldsymbol{0} \end{bmatrix} \boldsymbol{d}(t) = \boldsymbol{A}\boldsymbol{x}(t) + [\boldsymbol{\Gamma}_1 \ \boldsymbol{0}]\, \boldsymbol{d}(t) \quad (2.66)$$

$$\boldsymbol{y}(t) = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{C}_v \end{bmatrix} \boldsymbol{x}(t) + \begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{D}_v \end{bmatrix} \boldsymbol{d}(t) = \boldsymbol{C}\boldsymbol{x}(t) + [\boldsymbol{0} \ \boldsymbol{\Gamma}_2]\, \boldsymbol{d}(t) \quad (2.67)$$

$$\boldsymbol{e}(t) = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \boldsymbol{x}(t) - \begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \hat{\boldsymbol{x}}(t) = \boldsymbol{M}(\boldsymbol{x}(t) - \hat{\boldsymbol{x}}(t)) \quad (2.68)$$

Note, that $\boldsymbol{e}$ refers to the state estimation error $\boldsymbol{\Theta} - \hat{\boldsymbol{\Theta}}$. The design objective is the following

$$\boldsymbol{L} = \arg\min \|\boldsymbol{T}_{de}\|_\infty \quad (2.69)$$

The solution to this problem can be found in the H_∞ literature [60]. Assume that $\boldsymbol{\Gamma}_2\boldsymbol{\Gamma}_2^T$ is invertible, the solution is

$$\boldsymbol{L} = \boldsymbol{P}\boldsymbol{C}^T(\boldsymbol{\Gamma}_2\boldsymbol{\Gamma}_2^T)^{-1} \quad (2.70)$$

where $\boldsymbol{P}$ is the solution of the algebraic Riccati's equation

$$\boldsymbol{A}\boldsymbol{P} + \boldsymbol{P}\boldsymbol{A}^T + \boldsymbol{\Gamma}_1\boldsymbol{\Gamma}_1^T - \boldsymbol{P}\left[\boldsymbol{C}^T(\boldsymbol{\Gamma}_2\boldsymbol{\Gamma}_2^T)^{-1}\boldsymbol{C} - \frac{1}{\gamma^2}\boldsymbol{M}^T\boldsymbol{M}\right]\boldsymbol{P} = 0 \quad (2.71)$$

Once $\boldsymbol{L}$ is computed,

$$||\boldsymbol{T}_{de}||_\infty < \gamma \quad (2.72)$$

and the nonlinear form (2.63) is used for STR fault detection and isolation. It should be outlined that the IMU/IMU consistency check done at the lower level enables to discard IMU failures, leading this technique suitable for STR fault diagnosis. For residual evaluation, the test is applied to each component of $\boldsymbol{r}_\Theta$ and the decision making is done through a threshold based approach, i.e., if the GLR test is higher that a given threshold, then a Boolean is set. Due to the definition of $\boldsymbol{r}_\Theta$ in (2.63), the isolation of the faulty axis of the STRs is implicit. In order to illustrate an IMU/STR fault, Fig. 2.16 (left) considers a drift in the first axis of the STR, i.e., φ. Figure 2.16 (right) shows how this drift affect the quaternion measure.

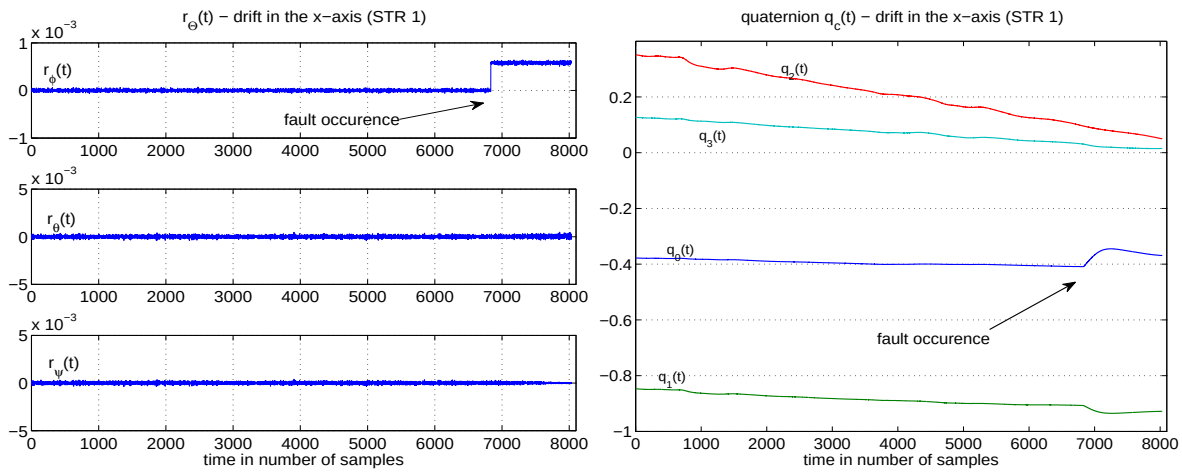


Figure 2.16 – Sensor drift in the STR (left) and the corresponding quaternion (right)

2.3.2 Description of the Set of Detection Functions at the Safety Monitoring Level

The higher level (level 3) is concerned by the thruster/IMU and wheel/tachometer consistency checks. At this level, it is assumed that all sensor faults have been detected and accommodated by the lower levels, so that all measures are deemed to be reliable.

As explained previously, Chapters 3 and 4 are dedicated to the problem of thruster fault detection, isolation and accommodation. So this problem is not considered here, since it is extensively discussed in the next chapters.

The wheel/tachometer consistency check, it is based on the following principle: since each wheel is equipped by a velocity sensor, namely a tachometer, that performs the measurement Ω_w, the following relation provides a residual dedicated to each wheel (isolation is thus immediate)

$$r_w(t) = J_w \frac{d\Omega_w(t)}{dt} - T_w(t) \tag{2.73}$$

In this equation, J_w is the inertia of the considered wheel and T_w is the (controlled) torque requested to deliver by the wheel. For decision making, a simple threshold–based approach has been revealed to be sufficient.

The higher level, level 4, is concerned by the check of the chaser spacecraft trajectory and velocity with respect to corridors and collision risk. During the last phases of the rendezvous (hopping and terminal rendezvous approach), the trajectory shall be kept within predefined corridors. Two corridors are defined: a smaller inner corridor with a slope at 8% that is used to trigger a corrective manoeuvre, and a wider corridor with a slope at 10% including the smaller one, that is used to trigger a collision avoidance maneuver. Figure 2.17 (left) shows the shape of the two corridors with the nominal trajectory of the chaser spacecraft. The corridors are centered on the approach direction and they have a conical shape. Similarly, the velocity of the chaser spacecraft is monitored. The capture velocity and the nominal velocity requirements of the chaser are illustrated on the Fig. 2.17 (right). If the chaser velocity exceeds the requirements (velocity along the capture axis between 5 cm/s and 15 cm/s and along the other axes, below 4 cm/s), a corrective maneuver is engaged.

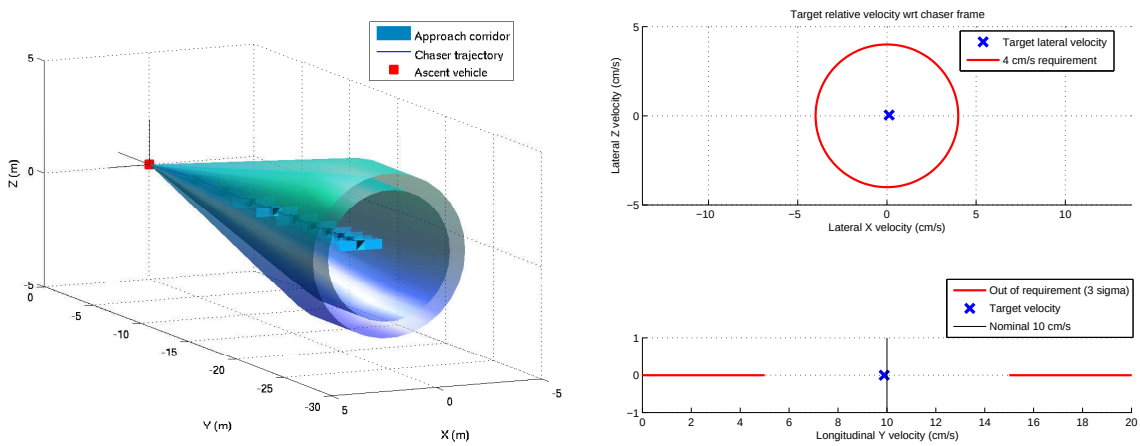


Figure 2.17 – The corridor shape during the rendezvous approach

Finally, the highest level, level 5, monitors the power to protect the overall systems and subsystems of the chaser against electrical failures and ground operation errors.

2.3.3 Thruster Fault Modelling

Following the fault management system described in the previous section, the main concern is now to develop FDI(R)/FTC algorithms for thruster faults to be implemented on level 3.

With regards to the possible faults occurring in the thruster-based propulsion system, the focus is on the so-called "open-type" (fully open and leaking thruster) and "closed-type" (blocked-closed and loss of efficiency) thruster faults. These faults have been defined in accordance with the industrial partners and follow both the TAS and ESA experiences. More precisely, the following thruster fault scenarios are considered:

- **Case 1: fully Open Thruster *(stuck open valve)***
  - provides maximum thrust regardless of the demanded command by TMF
- **Case 2: thruster Closing Itself *(blocked-closed)***
  - thruster does not generate any thrust regardless of the demand
- **Case 3: leakage *(bi-propellant residual leakage)***
  - leaking thruster of size $m_{leak}(t)$, starting from 0 and reaching the maximum leakage size $\hat{m}_{leak} > 0$ with a given slope $m_s > 0$, i.e., $m_{leak}(t) = \min\{m_s(t - t_f), \hat{m}_{leak}\}$, where t_f denotes the time of fault occurrence
- **Case 4: loss of Efficiency *(thrust loss)***
  - loss of efficiency of a particular thruster by a value $\hat{m}_{loss} > 0$.

Assuming no simultaneous faults, the considered thruster faults can be mathematically modelled in a multiplicative manner according to[4] (index "f" is used to outline the faulty case)

$$\begin{pmatrix} \boldsymbol{F}_f(t) \\ \boldsymbol{T}_f(t) \end{pmatrix} = \bar{\boldsymbol{B}}(\boldsymbol{I} - \boldsymbol{\Psi}(t))\tilde{\boldsymbol{u}}(t - \tau(t)) \tag{2.74}$$

with $\boldsymbol{\Psi}(t) = diag(\psi_1(t), \ldots, \psi_N(t))$, where $0 \leq \psi_k(t) \leq 1$, $\forall k \in \mathcal{S}_{all}$ are unknown. The health status of the kth thruster is modeled by $\psi_k(t)$ as follows

$$\psi_k(t) = \begin{cases} 0 & \textbf{if } \text{healthy} \\ 1 - \varphi_k(t)/\tilde{u}_k(t) & \textbf{if } \text{faulty} \end{cases}$$

where $\varphi_k(t)$ allows to consider all the four fault cases, mentioned earlier, as follows

$$\varphi_k(t) = \begin{cases} \max\{\tilde{u}_k(t), m_{leak}(t)\} & \textbf{if } \text{open-type} \\ (1 - \hat{m}_{loss})\tilde{u}_k(t) & \textbf{if } \text{closed-type} \end{cases}$$

In this formalism, $0 < \hat{m}_{leak} < 1$ models a leakage fault and $0 < \hat{m}_{loss} < 1$ an efficiency loss fault. It is obvious that $m_{leak}(t) = 1, \forall t \geq t_f$ refers to a fully open, and $\hat{m}_{loss} = 1$ to a blocked-closed thruster fault.

[4] It should be noted that a fault in one of the thrusters may generate an uncommented force/torque variation in all the 3 axes of the spacecraft.

The GNC unit, the failure detection and recovery management unit and the faults to be diagnosed being described, the main concern is now to derive the suitable mathematical models of the chaser motion. This is the purpose of the next section.

2.4 Modelling the Chaser Dynamics during the Rendezvous Phase

This section addresses the modelling the motion of the chaser spacecraft during the rendezvous phase. A linear relative position model and an attitude model of the chaser dynamics, that will be used in Chapters 3 and 4, are introduced for FDI purpose. These two models are able to describe the dynamics of the chaser spacecraft in both, fault-free and faulty situations. The relative position model is well known and mastered for control, but rarely used for fault diagnosis. The reason is quite simple: the attitude model "seems to be" more sensitive to thruster faults. The position model compared to the attitude model has the advantage that it is naturally robust against uncertainties of the inertia tensor and of the center of mass. In Fonod et al. [90], a sensitivity/robustness analysis campaign was performed to asses the reliability and the efficiency (in terms of detection times) of a position model-based fault detector. Encouraging results were obtained.

For the sake of brevity, only the necessary developments about the spacecraft dynamics modelling are introduced. The interested reader might refer to the extensive space literature about spacecraft modelling, see for instance [115, 256, 259, 296, 297].

2.4.1 Relative Position Model

The relative motion of one object with respect to another has gained a great interest over the past decades. The problem has been present since the use of Hill's equations [140]. The linearized Hill's equations around the null solution were introduced by Clohessy and Wiltshire [49] to analyze satellite rendezvous, and are now known as Hill–Clohessy–Wiltshire (HCW) equations [296]. The HCW equations propagate the relative position and velocity of the chaser with respect to the target in a Cartesian reference frame centered on a target object in a circular Keplerian orbit. These equations can also be used to form a linear time-invariant state space model of the relative dynamics. The key assumptions in the HCW equations are that: a) the two spacecraft are in close proximity, i.e., the distance between the chaser and target is very small compared with the distance to the centre of Mars, b) the target's orbit is near circular (orbital eccentricity $e = 0$) and c) the radial and out–of–plane separations are small [123].

Consider the illustration of the rendezvous between the chaser and target spacecraft around Mars given by Fig. 2.5. The translation motion of the chaser can be derived from the 2nd Newton law. To proceed, let a, m_c, $\mathcal{G}$, and m_M denote the radius of the circular orbit of the target, the mass of the chaser during the rendezvous, the universal gravitational constant and the mass of Mars, respectively. Then, the orbit of the rendezvous being circular, the velocity of the target is given by the relation

$$\sqrt{\frac{\mu}{a}} \tag{2.75}$$

where $\mu = \mathcal{G} \cdot m_M$[5]. Let us recall the definition of the local reference frame $\mathcal{F}_l = \{O_T; \vec{\boldsymbol{X}}_l, \vec{\boldsymbol{Y}}_l, \vec{\boldsymbol{Z}}_l\}$.

[5]Considered values: $\mathcal{G} \doteq 6.67384 \times 10^{-11}$ N.m^2 kg^{-2} and $m_M \doteq 6.4173 \times 10^{23}$ kg.

It is fixed at the center of the target O_T, with its $\vec{\boldsymbol{Z}}_l$ axis be perpendicular to the $\vec{\boldsymbol{X}}_l$ and $\vec{\boldsymbol{Y}}_l$ axis and oriented as shown in Fig. 2.5.

The linear velocity of the target is given by the relation $a.n$, where $n = \dot{\nu}$ stands for the uniform orbital rate of the target (hence the orbital period is $2\pi/n$). This velocity is given in the inertial frame $\mathcal{F}_i = \{O_M; \vec{\boldsymbol{X}}_i, \vec{\boldsymbol{Y}}_i, \vec{\boldsymbol{Z}}_i\}$, see Fig 2.5 if necessary. From the Kepler's third law it follows:

$$a.n = \sqrt{\frac{\mu}{a}} \Rightarrow n = \sqrt{\frac{\mu}{a^3}} \tag{2.76}$$

During the rendezvous phase, it is assumed that the chaser motion is due to the five following forces, all given in the local frame $\mathcal{F}_l = \{O_T; \vec{\boldsymbol{X}}_l, \vec{\boldsymbol{Y}}_l, \vec{\boldsymbol{Z}}_l\}$ (note that the rendezvous orbit is circular):

- the Mars attraction force $\vec{\boldsymbol{F}}_a = -m_c \frac{\mu}{((a+\xi)^2+\eta^2+\zeta^2)^{3/2}}\left((a+\xi)\vec{\boldsymbol{X}}_l + \eta\vec{\boldsymbol{Y}}_l + \zeta\vec{\boldsymbol{Z}}_l\right)$, where ξ, η, ζ denote the elements of the relative position vector $\boldsymbol{\rho} = [\xi, \eta, \zeta]^T$ of the chaser from the origin of the target frame O_T;
- the centripetal force $\vec{\boldsymbol{F}}_e = m_c\left(n^2(a+\xi)\vec{\boldsymbol{X}}_l + n^2\eta\vec{\boldsymbol{Y}}_l\right)$;
- the Coriolis force $\vec{\boldsymbol{F}}_c = m_c\left(2n\dot{\eta}\vec{\boldsymbol{X}}_l - 2n\dot{\xi}\vec{\boldsymbol{Y}}_l\right)$;
- the non-gravitational force (spatial perturbations) $\vec{\boldsymbol{F}}_p = F_{p\xi}\vec{\boldsymbol{X}}_l + F_{p\eta}\vec{\boldsymbol{Y}}_l + F_{p\zeta}\vec{\boldsymbol{Z}}_l$;
- the thruster-based propulsion system force $\vec{\boldsymbol{F}}_t = F_{t\xi}\vec{\boldsymbol{X}}_l + F_{t\eta}\vec{\boldsymbol{Y}}_l + F_{t\zeta}\vec{\boldsymbol{Z}}_l$. (This force vector is nothing else than the one given by (2.51) expressed in $\mathcal{F}_l$.)

Then, from the 2nd Newton law, it follows

$$\begin{cases} \ddot{\xi} = n^2(a+\xi) + 2n\dot{\eta} - \frac{\mu}{\left((a+\xi)^2+\eta^2+\zeta^2\right)^{3/2}}(a+\xi) + \frac{F_{t\xi}+F_{p\xi}}{m_c} \\ \ddot{\eta} = n^2\eta - 2n\dot{\xi} - \frac{\mu}{\left((a+\xi)^2+\eta^2+\zeta^2\right)^{3/2}}\eta + \frac{F_{t\eta}+F_{p\eta}}{m_c} \\ \ddot{\zeta} = -\frac{\mu}{\left((a+\xi)^2+\eta^2+\zeta^2\right)^{3/2}}\zeta + \frac{F_{t\zeta}+F_{p\zeta}}{m_c} \end{cases} \tag{2.77}$$

Because the distance between the target and the chaser, during the rendezvous, is negligible compared to the radius of the target orbit, i.e., $\|\boldsymbol{\rho}\| \ll a$, therefore it is possible to derive the HCW equations from (2.77) by means of a first order approximation of the nonlinear state space model[49]. Finally, by introducing the fault model (2.74) and the CPDE unknown time-varying delay $\tau(t)$, the translation motion of the chaser can be modeled in the target (local) frame $\mathcal{F}_l$, in both fault-free (i.e., $\boldsymbol{\Psi}(t) = 0$) and faulty (i.e., $\boldsymbol{\Psi}(t) \neq 0$) situations, according to the linear 6th order state space representation with state vector $\boldsymbol{x}_p = [\xi\ \eta\ \zeta\ \dot{\xi}\ \dot{\eta}\ \dot{\zeta}]^T$. It can be verified that from (2.77) it follows

$$\begin{cases} \dot{\boldsymbol{x}}_p(t) = \boldsymbol{A}_p\boldsymbol{x}_p(t) + \boldsymbol{B}_p\boldsymbol{R}(\boldsymbol{q}_t(t), \boldsymbol{q}_c(t))\boldsymbol{F}_f(t) + \boldsymbol{E}_{pp}\boldsymbol{F}_p(t) \\ \boldsymbol{y}_p(t) = \boldsymbol{C}_p\boldsymbol{x}_p(t) \end{cases} \tag{2.78}$$

where

$$\boldsymbol{A}_p = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 3n^2 & 0 & 0 & 0 & 2n & 0 \\ 0 & 0 & 0 & -2n & 0 & 0 \\ 0 & 0 & -n^2 & 0 & 0 & 0 \end{pmatrix}, \quad \boldsymbol{B}_p = \boldsymbol{E}_{pp} = \frac{1}{m_c} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \boldsymbol{C}_p = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

In (2.78), $\boldsymbol{q}_t \in \mathbb{H}$ and $\boldsymbol{q}_c \in \mathbb{H}$ stand for the attitude quaternion of the target and the chaser, respectively. These quaternions describe the orientation of the target body frame ($\boldsymbol{q}_t$) and the chaser body frame ($\boldsymbol{q}_c$) with respect to the inertial frame $\mathcal{F}_i$. The estimates $\hat{\boldsymbol{q}}_t$ and $\hat{\boldsymbol{q}}_c$ of these signals are assumed to be available on-board since they are computed online by the navigation unit, see Section 2.2. The quaternion-dependent rotation matrix $\boldsymbol{R}(\cdot)$ performs the projection of the three-dimensional force vector $\boldsymbol{F}_f$ from the chaser body-fixed frame on to the target frame $\mathcal{F}_l$, see its equivalence $\boldsymbol{F}_t$ in (2.77). Let us remind the reader that $\boldsymbol{F}_f$ denotes the forces due to the propulsion system of the chaser spacecraft that can be possibly faulty, see (2.74). The output vector $\boldsymbol{y}_p = \boldsymbol{\rho} = [\xi \ \eta \ \zeta]^T$ is the relative position of the two spacecrafts expressed in $\mathcal{R}_l$ and is assumed to be measured by the LIDAR device. Spatial disturbances (solar radiation pressure, gravity gradient and atmospheric drag) are represented by $\boldsymbol{F}_p$. Moreover, it is assumed that the navigation unit is decoupled from thruster faults. This is a reasonable assumption since, as previously explained, sensor faults are diagnosed and accommodated at the lowest level of the failure management unit.

2.4.2 Attitude Model

To fully describe the rotational motion of the chaser, dynamic and kinematic equations of motion are required [256, 259, 295–297]. The attitude control system works in a target pointing mode, which means that the chaser keeps one face of the spacecraft pointed to the target and maintains it during the whole rendezvous phase (see Fig 2.18 for illustration).

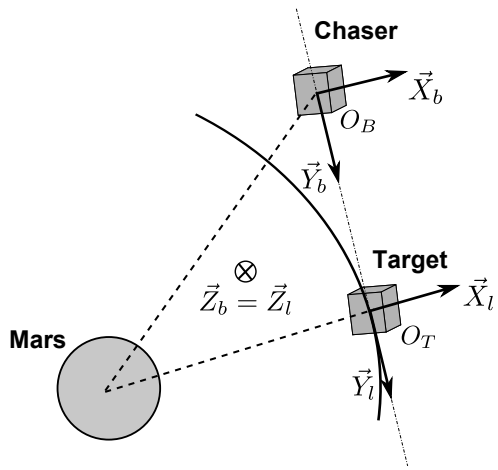


Figure 2.18 – Chaser attitude target pointing mode

Let's consider the spacecraft as a rigid body, the rotational motion of this body caused by an applied moment (sum of all external torques acting on the body) can be derived in the inertial

frame $\mathcal{F}_i$ from the Euler's second law. This law says that the time derivative of the angular momentum $\boldsymbol{L}$ of any rotating body equals the sum of all applied torques about its center of mass, i.e.,

$$\dot{\boldsymbol{L}} = \sum_k (\boldsymbol{T}_k)^{\mathcal{F}_i} \tag{2.79}$$

where $(\boldsymbol{T}_k)^{\mathcal{F}_i}, k = 1, 2 \ldots$ are the external torques acting on the body center of mass and given in $\mathcal{F}_i$. In practice, it is more convenient to simply express $\boldsymbol{L}$ in a frame of reference whose axes are fixed to the rotating body. Therefore, the mathematical model of the chaser rotational dynamics (flex modes and slosh phenomena are not considered) in the body-fixed reference frame $\mathcal{F}_b = \{O_B; \vec{\boldsymbol{X}}_b, \vec{\boldsymbol{Y}}_b, \vec{\boldsymbol{Z}}_b\}$ (the center of this frame is fixed to the center of mass of the chaser and their axes are parallel to those of the local target reference frame) can be derived from (2.79)

$$\dot{\boldsymbol{\omega}}(t) = \boldsymbol{J}^{-1}(\boldsymbol{T}(t) + \boldsymbol{T}_p(t)) - \boldsymbol{J}^{-1}\boldsymbol{\omega}(t) \times \boldsymbol{J}\boldsymbol{\omega}(t) \tag{2.80}$$

where $\boldsymbol{\omega} = [p, q, r]^T$ is the angular velocity vector of the frame $\mathcal{F}_b$ relative to the inertial frame $\mathcal{F}_i$, and $\boldsymbol{J} \in \mathbb{R}^{3\times 3}$ is the inertia dyadic about the chaser CoM. In (2.80), $\boldsymbol{T}$ and $\boldsymbol{T}_p$ describe the external torques about the CoM that are due to the thrusters (i.e., $\vec{\boldsymbol{T}}$) and due to the orbital perturbations (i.e., $\boldsymbol{T}_p$). Note that, in (2.80), both $\boldsymbol{\omega}$ and $\boldsymbol{J}$ are given in $\mathcal{F}_b$.

Using the individual rotation matrices from an Euler's rotation of type (3,2,1), it is possible to express the relation between the rotational velocities $\boldsymbol{\omega}$ and the rate of the Euler angles $\dot{\boldsymbol{\Theta}} = [\dot{\varphi}\ \dot{\theta}\ \dot{\psi}]^T$. Its inverse relationship then describes the kinematic equations for the attitude [296]

$$\dot{\boldsymbol{\Theta}}(t) = \frac{1}{\cos(\theta)} \begin{bmatrix} \cos(\theta) & \sin(\varphi)\sin(\theta) & \cos(\varphi)\sin(\theta) \\ 0 & \cos(\varphi)\cos(\theta) & -\sin(\varphi)\cos(\theta) \\ 0 & \sin(\varphi) & \cos(\varphi) \end{bmatrix} \boldsymbol{\omega}(t) \tag{2.81}$$

Note that (2.81) becomes singular when the pitch angle approaches $\theta = \pi/2 \pm k\pi, k \in \mathbb{Z}^+$. A solution to avoid singularities in the kinematics equations is to describe the attitude by by quaternion representation, see Appendix A.

Considering that, during the rendezvous phase, the chaser spacecraft is controlled around the equilibrium points[6] $\boldsymbol{\Theta} = \boldsymbol{\Theta}_0$ (with $\theta \neq \pm 90°$) and $\boldsymbol{\omega} = \boldsymbol{0}$, choosing $\boldsymbol{x}_a = [\varphi\ \theta\ \psi\ p\ q\ r]^T$ as the attitude model state vector and by introducing the fault model (2.74) together with the CPDE unknown delay $\tau(t)$, the rotational motion (both kinematics and dynamics) of the chaser can be derived by means of a first-order approximation of the nonlinear equations (2.80) and (2.81) around the equilibrium points, in both fault-free (i.e., $\boldsymbol{\Psi}(t) = 0$) and faulty (i.e., $\boldsymbol{\Psi}(t) \neq 0$) situations, according to the following 6th order linear state space model

$$\begin{cases} \dot{\boldsymbol{x}}_a(t) = \boldsymbol{A}_a\boldsymbol{x}_a(t) + \boldsymbol{B}_a\boldsymbol{T}_f(t) + \boldsymbol{E}_{ap}\boldsymbol{T}_p(t) \\ \boldsymbol{y}_a(t) = \boldsymbol{C}_a\boldsymbol{x}_a(t) \end{cases} \tag{2.82}$$

where matrices $\boldsymbol{A}_a, \boldsymbol{B}_a = \boldsymbol{E}_{ap}$ and $\boldsymbol{C}_a$ result from the linearization process around $\boldsymbol{x}_{a0} = [\boldsymbol{\Theta}_0\ \boldsymbol{0}]$, i.e.

$$\boldsymbol{A}_a = \begin{pmatrix} \boldsymbol{0} & \boldsymbol{I} \\ \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}, \quad \boldsymbol{B}_a = \boldsymbol{E}_{ap} = \begin{pmatrix} \boldsymbol{0} \\ \boldsymbol{J}^{-1} \end{pmatrix}, \quad \boldsymbol{C}_a = \boldsymbol{C}_p$$

[6] This is a reasonable assumption from practical point of view since the chaser spacecraft works in an attitude target pointing mode and the distance between the two spacecrafts is very small ($\leq$ 20 m), thus the pointing guidance is a straight line like.

Let us recall the reader that $\boldsymbol{T}_f$ denotes the torques due to the propulsion system of the chaser spacecraft that can be possibly faulty, see (2.74).

The attitude model (2.82) and the position model (2.78) will be used in the following chapters to design robust FDIR/FTC solutions.

2.5 Conclusion

This chapter described the Mars Sample Return mission, its rendezvous phase and the vehicles involved in the mission (i.e., the target and chaser spacecraft). It described the GNC unit that is in charge to control the chaser during the rendezvous phase and the failure management unit that is in charge to detect failures and to engage corrective maneuvers. It is shown how the FDIR and FTC solutions investigated in the next chapters, can be integrated in the failure management unit. This chapter further addressed the models of the chaser spacecraft dynamics (relative position between the chaser and the target and chaser attitude) that is used in the following chapters to design model-based FDIR/FTC solutions. Modelling of the chaser spacecraft thruster-based propulsion is also considered to outline the effect of the faults. All investigated fault scenarios are discussed, too.

All models and functions described in this chapter have been embedded in a "high-fidelity" industrial simulator developed by TAS. The simulator is implemented in the MATLAB®/Simulink® environment. It consists of a nonlinear model of the rigid body dynamics of the chaser and target in a Mars orbit. The simulator assumes that the Mars planet is in a Keplerian orbit about the sun. The chaser and target orbits around the Mars are modelled using Gauss' equations, with the gravitational field of Mars calculated using a spherical harmonic expansion with the Mars50c coefficients [123]. The attitude dynamics are modelled assuming that the target and chaser are rigid bodies [89, 259]. The effects of external disturbances (earlier referred as orbital perturbations) due to gravity gradient, solar radiation pressure and atmospheric drag (assuming an exponential atmospheric model) are also included in the simulator. A number of uncertainties are considered in the simulator, from the variations of the initial conditions, parametric uncertainties in the different components of the spacecraft (e.g., mass, CoM, moment of inertia, thrusters, see Table 2.3), up to navigation uncertainties (on LIDAR, STR, IMU).

This simulator will be considered to validate the theoretical developments proposed in the next chapters in which model-based FDIR and FTC solutions are investigated. The solutions that will be proposed, fit the fault management architecture that is described in this chapter. More precisely, Chapter 3 will address a FDIR solution that can be integrated in the level 3, the recovery principle being exactly those used by the SHM, i.e., switching to a redundant set of equipments. Chapter 4 will also address a more enhanced solution since it relies on an active FTC approach. However, since an active FTC approach involves an FDI unit, it is guaranteed that the FDI part can be embedded at level 3. In other words, all solutions proposed in this thesis must be understood to be an integral part of the overall failure management unit currently developed by Thales Alenia Space for the MSR mission.

Chapter 3

Advanced Model-based FDIR Solution for the Baseline MSR Thruster Configuration

"Prepare your proof before you argue."
— Jewish proverb

In this chapter, the design and implementation of two distinct model-based FDIR techniques to detect, isolate and accommodate (recover) a single thruster fault affecting the chaser spacecraft propulsion system are addressed. The first approach is based on the position model whereas the second approach is based on a pure attitude model. Both techniques focus on the robustness issue against the unknown time-varying delays induced by the propulsion drive electronics and uncertainties on thruster rise times. A complete description of a robust residual generation design approach based on eigenstructure assignment technique is discussed in details. Computational procedure and implementation issues of the FDI scheme design are carefully discussed. Particular novelty of the work presented in this chapter is the development of a new method for estimating the unknown input directions used to enhance robustness property of the diagnosis scheme. The fault accommodation is achieved by employing the additional hardware redundancy in the thruster-based propulsion system. Finally, Monte Carlo results demonstrate feasibility and efficiency of the proposed FDI schemes. Carefully selected performance and reliability indices allow to compare the effectiveness of both approaches. Recovery aspects are also studied.

3.1 Problem Statement and Motivation

In space systems, fault tolerance is usually achieved by FDIR (Fault/Failure Detection Isolation and Recovery). This approach relies on hardware-based redundancy in actuators and sensors. At the present time, the fault detection task of in-flight spacecraft is based on cross, consistency, and limit-value checks, respectively. Monitored variables are verified with respect to certain tolerances of nominal values. Alarms are triggered if the thresholds are exceeded. Different architectures for an industrial state of practice FDIR have been suggested in the literature, see [189, 214, 217, 245] for good surveys.

Actuator faults are detected at higher level through consistency checks, see discussion in Section 2.3. The classical thruster fault detection is based on the comparison of the commanded torque and force with the IMU measurements. An alarm is raised when a thruster is opened during a too long time. Fixed thresholds are used for recognition of out-of-tolerance condition [214].

Space literature reports that conventional FDIR techniques (present-day techniques) are suffering from significant shortcomings, like often missing isolation capabilities of faults on-board [214]. The classical FDIR approach for a thruster configuration as in Fig. 3.2 consists of a "half satellite" strategy, where only fault detection is performed on-board [214]. If a fault is detected, the nominal thruster set is switched to a redundant one (see Fig. 3.1) and the spacecraft mode is changed to a predefined system safe mode, waiting for a ground intervention. However, in mission critical phases like rendezvous capture/docking phase, the transition to safe mode could possibly lead to collision with the target, thus the safe mode is switched off during the rendezvous phase and a collision avoidance maneuver is triggered rather.

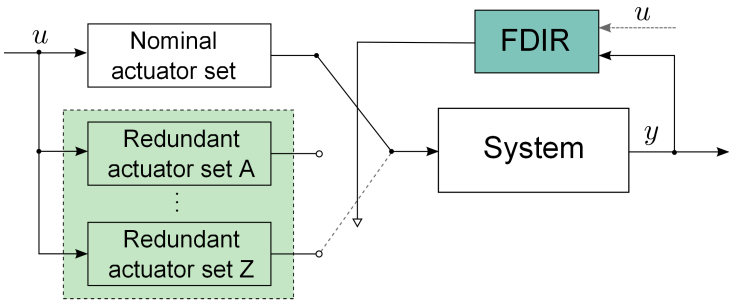


Figure 3.1 – "Half satellite" strategy for thruster faults

In some cases, "industrial approaches" exist for on-board fault isolation. For instance:

- One possibility is through the use of specialized pressure and temperature sensors in the nozzle of the thruster. This, however, comes at the price of extra mass, cost and complexity [245]. Therefore, only methods allowing to perform thruster FDIR using only additional software and/or hardware already on-board are considered in this chapter.
- Another industrial method is based on sending thruster commands (in addition to the command produced by the control law) to all thrusters and assuming that the faulty thruster has no effect on the spacecraft dynamics. Then, the observation of the IMU measurements over a some period of time enables to isolate the failed thruster. This approach, however, has several drawbacks, like extra fuel consumption, degraded control accuracy and it might not work for closed-type thruster failures (stuck closed or thrust loss). All these shortcomings discourage the usage of this method for close range rendezvous.

In non-critical mission phases, common (industrial) methods are well-proven, but for critical mission phases like rendezvous and docking, advanced model-based FDIR techniques shall be particularly developed to cope with the necessary robustness/stability of the spacecraft control, the necessary trajectory dynamics and the vehicle nominal operation. To ensure normal operation, real-time fault diagnosis is essential to provide information for the spacecraft to accommodate the fault in time [289].

The enhanced model-based FDIR approaches take advantage of the available on-board input-output relations, analytical and informational redundancy. The expected benefits of these meth-

ods are to provide additional and more precise fault indicators to assess the occurred faulty situation. In [289], a gap analysis has been discussed on drawback of classical FDIR methods in deep space applications. It suggests that in critical mission phases, an interesting approach would be to assist the innovative FDIR methods of the system with traditional methods [289].

Obviously, there is a natural tendency to take profit from the continuously increasing spacecraft on-board computational resources that sets the scene for the application of more sophisticated and powerful FDIR techniques, based on modern estimation/decision tools. These advanced techniques enable to respond to faults in a timely manner, increase spacecraft autonomy and thus offering prospect of reducing the overall operational cost. The FDIR approach proposed in the next sections follows this philosophy. As explained in the previous chapter, the focus of this study is on thruster faults, sensor faults being assumed to be diagnosed and accommodated at lower levels.

Baseline MSR Thruster Configuration

The baseline MSR thruster configuration that is considered in the following developments was designed for full redundancy. Particularly it means that for this configuration, the chaser is equipped with a propulsion system composed of 2×8 thrusters arranged in two sets. The nominal set 'A' is used for the nominal vehicle control and the redundant set 'B' is reserved for the recovery actions, i.e., the set 'A' is switched off and the set 'B' becomes active as soon as a fault has been detected. The thruster configuration is illustrated in Fig. 3.2.

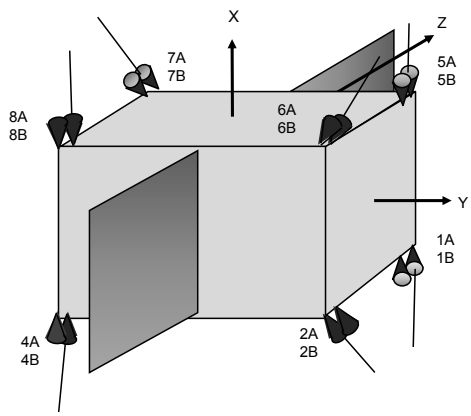


Figure 3.2 – Baseline MSR thruster configuration of the chaser spacecraft

The design of this configuration was driven by the following industrial aspects:

a) The need to minimize the interaction of the thrusters plume with payloads, optical sensors, solar arrays or a chaser first stage that is jettisoned before rendezvous operation.

b) The need to minimize the number of thrusters while ensuring a full redundancy: A consequence is that there is no need to isolate the thruster fault. Whatever the thruster fault, the recovery consists in switching to the redundant set.

c) The need to cope with center of mass evolutions during the chaser life.

This configuration enables a full 6 DOF control (attitude and translation) using any of the thruster set (nominal or redundant). As mentioned earlier, the propulsion system uses only 8

of the 16 thrusters to control the spacecraft in normal operation. Thus, for the FDI design and implementation in the next section, only the nominal thruster set 'A' is considered and the total number of (active) thrusters will be denoted by $N = 8$. It should be noted, that every thruster in the configuration of Fig. 3.2 has a partner thruster that produces a force in exactly the opposite direction and torque in the exactly same direction, see Fig. 3.3 for illustration.

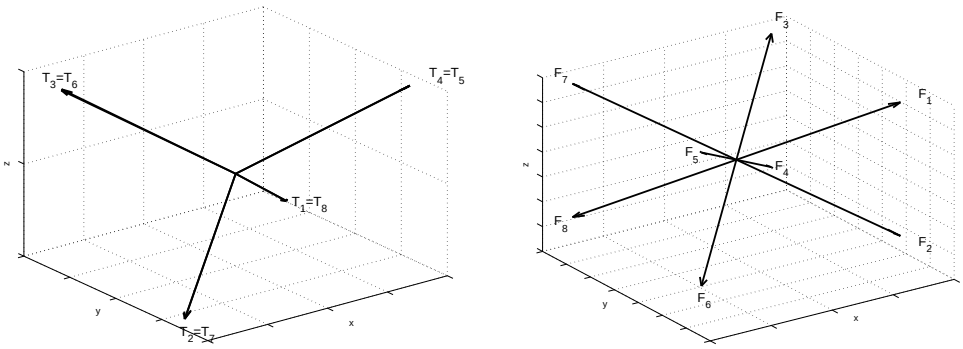


Figure 3.3 – Torque directions (left) and force directions (right)

Justification of the FDIR Approach

The nominal thrusters set of the baseline configuration has just enough thrusters to produce any necessary force and torque in order to cope with the demand of the 6DOF control law (in normal operation). So this configuration is in some sense "optimal", meaning that even if only a single thruster fails, the nominal set may become underactuated[1]. This, however, cannot be checked with the classical controllability test. For example, in the case of a single fault (i.e., 7 >DOF), the controllability test will indeed result as positive (controllable). This misinterpretation is due to the fact that all thrusters are unilateral, meaning that they cannot produce negative thrust and therefore actuator saturation limits must be considered for such a test.

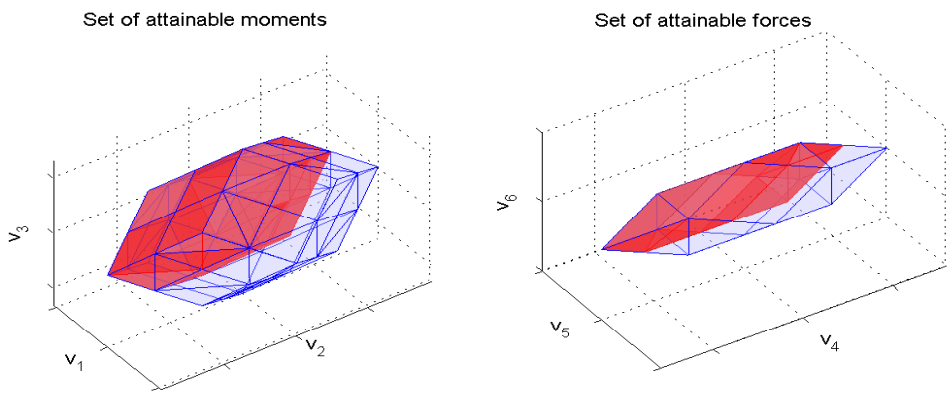


Figure 3.4 – Set of attainable moments (left) and forces (right) using all the 8 nominal thrusters (blue polyhedron) and using only 7 thrusters (red polyhedron). In both cases the thruster limits are taken into account.

Taking into account thruster limits, Fig. 3.4 demonstrates the set of attainable forces/moments

[1]For instance, if a single thruster suffers from a partial (small) loss of efficiency, the spacecraft might still perform close to the nominal case, therefore "may become underactuated".

using all the 8 nominal thrusters (Ω_a^8) as well as the subset of this set when thruster No.1 is not considered ($\Omega_a^{1/8} \subset \Omega_a^8$). This figure clearly illustrates that a big portion of nominally attainable forces/moments (quasi control authority) is lost if only $N - 1 = 7$ thrusters are considered to control the spacecraft. It can be also verified by means of closed-loop simulations that, if any combination of 7 thrusters is considered for control, the GNC performance is very degraded and the required rendezvous objectives cannot be met. This justifies the need for an FDIR approach instead of an FTC one, i.e., an approach where fault accommodation is performed by using some thrusters from the redundant thruster set 'B'.

From the above reasoning, it becomes clear that the crucial element of the FDIR approach is the FDI unit. It decides which component of the system or subsystem is faulty. Then one activates the redundant sub-system in order to recover the initial performance. That is what "R" means in the acronym FDIR.

3.2 Robust FDI Scheme Design

Due to the central role of the FDI scheme in the FDIR architecture, robustness issues must be rigorously addressed. In this section, two model-based FDI schemes are presented with enhanced robustness against the uncertain time-varying delay $\tau(t)$ which, as mentioned earlier, aims at modelling the uncertainties on the thruster rise times and delays induced by the CPDE device, see Section 2.2.3 for discussion about these uncertainties.

The first FDI scheme is based on the position model (2.78) and the second one uses the attitude model (2.82). For both schemes, decision making is done using the GLR test (see Appendix B) and the isolation task is achieved by evaluating a cross-correlation like criterion between the component of the residual and the commanded thruster opening intervals. Finally, fault recovery is based on redirecting the control input to the redundant thruster and switching off the faulty thruster with a dedicated closing mechanism.

3.2.1 Overview of the Time-delay Problematic

Considering FDI of time-delay systems, only limited results have been developed in recent years in the literature. Among the contributions, an UIO was designed for fault detection of state-delayed systems with "known" delays [300]. The well known parity space approach was extended for fault detection of retarded time-delay systems [166]. In [62, 150], a two-objective optimization approach was considered for LTI systems, again considering constant time-delays aiming at a formulation of the optimization problem as: enhancing sensitivity of the residual to faults and at the same time suppressing the undesirable effects of unknown inputs and uncertainties in $\mathcal{L}_2$-gain sense. In [152], a robust fault diagnosis approach based on an adaptive observer was developed for uncertain continuous LTI systems with multiple discrete time-delays in both states and outputs. Recently, a geometric approach for FDI of retarded and neutral time-delay systems was developed [194]. Problem of robust fault detector design for a class of LTI systems with some nonlinear perturbations and mixed neutral and discrete time-varying delays is investigated in [160] using a descriptor technique, Lyapunov-Krasovskii functional and a suitable change of variables.

Often, uncertain time-varying delays occur in the input channels of the system. This is also the case of the thruster-based propulsion system of the chaser spacecraft considered in this thesis. Dealing with FDI, one of the main difficulty lies in the fact that the uncertainty caused by such delays is unstructured. Therefore, robustness cannot be achieved by applying directly existing robust unknown input (disturbance) decoupling approaches directly. There is an important assumption for all such approaches, i.e., the distribution matrix through which the uncertainty affects the system state must be known. However, a generalized approach to obtain the distribution matrix is still lacking, see e.g., [222, 230] for further discussion about this problematic.

This chapter provides a solution to this problems by introducing a Cayley-Hamilton's theorem-based and h-order Taylor series expansion-based polytopic transformations, the influence of the time-varying delay (uncertainty) on the system state is summarized as an unknown input. This is (thought to be) a novel approach of estimation of the distribution matrix related to the uncertain time-varying input delay which is a prior condition for the application of unknown inputs decoupling techniques. For residual generation, Patton and Chen shown that by assigning the eigenstructure of an observer-based scheme, the residuals can be decoupled from these unknown inputs [222]. The solutions investigated here follow this strategy. More precisely, some left eigenvectors of the observer are assigned to be orthogonal to the unknown input entry directions (columns of the distribution matrix) and thus providing a robust fault detector.

3.2.2 Problem Formulation

Consider the position model (2.78) and the attitude model (2.82) derived in the previous chapter. Due to the quaternion-based rotation matrix $\boldsymbol{R}(\boldsymbol{q}_t, \boldsymbol{q}_c)$ (for position model only) and due to the presence of the time-varying delay $\tau(t)$ in the control signal $\tilde{\boldsymbol{u}}$, suitable model transformations and manipulations have to be addressed so that both models are in a general and unified form (1.39) (see Chapter 1) that is suitable for the unknown input decoupled residual approach using the EA technique. This is the purpose of the following developments.

To proceed, consider the relative position model (2.78), the multiplicative fault model (2.74) and the model (2.51) relating the thruster ON-times $\tilde{\boldsymbol{u}}$ with the forces $\vec{\boldsymbol{F}}$ (due to the thrusters). Then, a new system input vector $\boldsymbol{u}_p \in \mathbb{R}^3$ can be defined according to

$$\boldsymbol{u}_p(t) = \boldsymbol{R}(\boldsymbol{q}_t(t), \boldsymbol{q}_c(t))\boldsymbol{B}_F\tilde{\boldsymbol{u}}(t - \tau(t)) \tag{3.1}$$

and the fault model can be approximated in terms of an additive fault vector $\boldsymbol{f}_p \in \mathbb{R}^3$ as follows

$$\boldsymbol{f}_p(t) = -\boldsymbol{R}(\boldsymbol{q}_t(t), \boldsymbol{q}_c(t))\boldsymbol{B}_F\boldsymbol{\Psi}(t)\tilde{\boldsymbol{u}}(t - \tau(t)) \tag{3.2}$$

where $\boldsymbol{B}_F \in \mathbb{R}^{3\times 8}$ is the lower block of the thruster configuration matrix $\bar{\boldsymbol{B}}$ related to the considered thruster configuration, see (2.53) and Fig. 3.2 if necessary. This type of approximation is widely used in the literature. The interested reader can refer to Isermann [145] and Frank et al. [97] for a discussion of such an approximation.

Considering (2.78) together with (3.1) and (3.2), the relative position model which suits the FDI

scheme design purposes can be written in the following form

$$\begin{cases} \dot{\boldsymbol{x}}_p(t) = \boldsymbol{A}_p\boldsymbol{x}_p(t) + \boldsymbol{B}_p\boldsymbol{u}_p(t) + \boldsymbol{E}_{pf}\boldsymbol{f}_p(t) \\ \boldsymbol{y}_p(t) = \boldsymbol{C}_p\boldsymbol{x}_p(t) \end{cases} \tag{3.3}$$

where $\boldsymbol{f}_p$ is acting on the state via a constant distribution matrix $\boldsymbol{E}_{pf} = \boldsymbol{B}_p$. The output vector is defined as $\boldsymbol{y}_p = [\xi\ \eta\ \zeta]^T$ (the relative position between the chaser and the target) and the input vector is defined as the delayed control signals (3.1) given in the local frame $\mathcal{F}_l$.

Taking similar steps as for the position model, the attitude model (2.82) can be rewritten according to

$$\begin{cases} \dot{\boldsymbol{x}}_a(t) = \boldsymbol{A}_a\boldsymbol{x}_a(t) + \boldsymbol{B}_a\boldsymbol{u}_a(t) + \boldsymbol{E}_{af}\boldsymbol{f}_a(t) \\ \boldsymbol{y}_a(t) = \boldsymbol{C}_a\boldsymbol{x}_a(t) \end{cases} \tag{3.4}$$

where $\boldsymbol{f}_a \in \mathbb{R}^3$ stands for the additive fault vector, $\boldsymbol{E}_{af} = \boldsymbol{B}_a$ and $\boldsymbol{u}_a \in \mathbb{R}^3$ is the new input vector defined as

$$\boldsymbol{u}_a(t) = \boldsymbol{B}_T\tilde{\boldsymbol{u}}(t - \tau(t)) \tag{3.5}$$

$$\boldsymbol{f}_a(t) = -\boldsymbol{B}_T\boldsymbol{\Psi}(t)\tilde{\boldsymbol{u}}(t - \tau(t)) \tag{3.6}$$

with $\boldsymbol{B}_T \in \mathbb{R}^{3\times 8}$ being the upper block of the MSR thruster configuration matrix $\bar{\boldsymbol{B}}$. The output vector is defined as $\boldsymbol{y}_a = [\varphi, \theta, \psi]^T$ (the chaser attitude Euler's angles) and the input vector is defined as the delayed control signals given by (3.5). The model (3.4) is now suitable for the FDI filter design technique proposed in the next section and has exactly the same structure as the position model given by (3.3).

From (3.3) and (3.4) it is clear that both models admit the following general description of a continuous LTI system

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{E}_f\boldsymbol{f}(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{3.7}$$

where $\boldsymbol{x} \in \mathbb{R}^{n_x}$, $\boldsymbol{u} \in \mathbb{R}^{n_u}$, $\boldsymbol{y} \in \mathbb{R}^{n_y}$, and $\boldsymbol{f} \in \mathbb{R}^{n_f}$ is system state, system input, measurement, and unknown fault vector, respectively. The quadruplet $\{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{E}_f\}$ represents the state-space matrices either of the position (3.3), or the attitude (3.4) model. It is assumed that all considered faults $\boldsymbol{f}$ are detectable (see [190] for more details on fault detectability) and that the pair $(\boldsymbol{A}, \boldsymbol{C})$ is observable.

Now, consider the TMF described in Section 2.2.3 in Chapter 2. Since the TMF generates the thruster opening times equidistantly with a fixed sampling interval $T > 0$, the system (3.7) can be seen as a discrete-time controlled system. Modelling of continuous time systems with digital control and delayed control input was for example introduced in [195]. Under the assumption that $\tau(t)$ is constant during each control cycle "k", i.e., $\tau(t) = \tau(k), \forall t \in [kT, (k+1)T)$, the same philosophy can be employed here.

Noting that the control signal $\tilde{\boldsymbol{u}}(k)$, generated at time $t = kT, k \in \mathbb{Z}^+$, arrives to the actuator at time instant $t = kT + \tau(k)$ (i.e., with the delay of $\tau(k)$). It is then kept unchanged by the zero-order-hold until the next control signal arrives. Noting that the time-varying delay $\tau(k)$ is upper bounded, i.e., $\tau(k) \leq \bar{\tau}, \forall k \in \mathbb{Z}^+$, it follows that the system input, affected by delays, is given by

$$\boldsymbol{u}(t) = \begin{cases} \boldsymbol{u}_c(k-1), & t \in [kT, kT + \tau(k)) \\ \boldsymbol{u}_c(k), & t \in [kT + \tau(k), (k+1)T) \end{cases} \tag{3.8}$$

where $\boldsymbol{u}_c$ depends on the considered model so that

$$\boldsymbol{u}_c(k) = \begin{cases} \boldsymbol{R}(\boldsymbol{q}_t(k), \boldsymbol{q}_c(k))\boldsymbol{B}_F\tilde{\boldsymbol{u}}(k), & \textbf{if } \text{position model is considered} \\ \boldsymbol{B}_T\tilde{\boldsymbol{u}}(k), & \textbf{if } \text{attitude model is considered} \end{cases} \tag{3.9}$$

The residual generation problem under the unknown input decoupling constraint can then be formulated as follows.

Problem 3.1. *Design a discrete time residual generator of the form*

$$\boldsymbol{r}(z) = \boldsymbol{H}_y(z)\boldsymbol{y}(z) + \boldsymbol{H}_u(z)\boldsymbol{u}_c(z) \tag{3.10}$$

with $\boldsymbol{H}_y/\boldsymbol{H}_u$ being observer-based transfer functions, such that the residual signal $\boldsymbol{r}$ lends robustness against the uncertain delay $\tau(k)$.

To solve Problem 3.1, the influence of the uncertain parameter $\tau(k)$ is first approximated as an unknown input which acts on the system state via a constant distribution matrix. This unknown input is then decoupled by means of the left EA technique. In the following, two approaches are proposed, the first uses a Cayley-Hamilton theorem-based, whereas the second considers a h-order Taylor series expansion-based polytopic transformation of $\tau(k)$. As already mentioned, the decision making is done using the GLR test and the isolation is performed using a cross-correlation like test between the residual and the commanded thruster opening intervals.

Figure 3.5 illustrates general overview of the proposed FDI scheme based on the position model together with its internal and external signals. The red coloured blocks are concerned with the robust residual generation whereas the yellow coloured blocks corresponds to the evaluation function of the residual (fault detection and isolation). The green coloured blocks represent the necessary signal transformations for the FDI. The explicit meaning and operation of each particular block in Fig. 3.5 will be explained in details in the following developments.

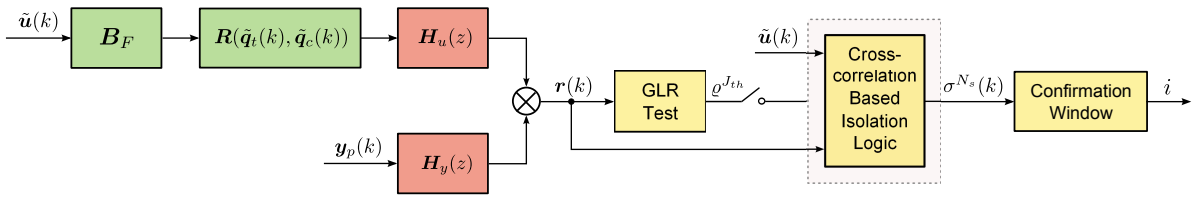


Figure 3.5 – Position model-based FDI scheme

Similarly as for the position model, Fig. 3.6 illustrates the general overview of the proposed FDI scheme based on the attitude model. The differences and advantages of either schemes will be discussed in the sequel.

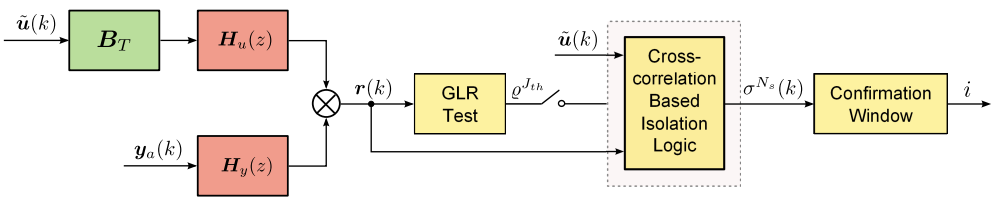


Figure 3.6 – Attitude model-based FDI scheme

Remark 3.1. *It is important to note that spatial disturbances (perturbations) $\vec{\boldsymbol{F}}_p$ and $\vec{\boldsymbol{T}}_p$ are omitted from* (3.3) *and* (3.4)*. The reason is simple. Since exact disturbance (unknown input) decoupling techniques are considered in the following developments and since the spatial disturbances act on the state via the same distribution matrix (in the same directions) as those of the inputs and thruster faults, i.e., $\boldsymbol{B}_p = \boldsymbol{E}_{pf} = \boldsymbol{E}_{pp}$ and $\boldsymbol{B}_a = \boldsymbol{E}_{af} = \boldsymbol{E}_{ap}$, so decoupling these disturbances means decoupling the inputs and faults, too. This is a well know issue (fact) in the space community when considering robust fault diagnosis problem against spatial disturbances*[2]*. Robustness against these disturbances can be checked a-posteriori, for instance using a huge number of Monte Carlo simulations.*

3.2.3 Uncertainty Transformation

Assume that $\tau(k)$ can be partitioned as follows

$$\tau(k) = lT + \delta(k) \leq \bar{\tau} \tag{3.11}$$

where $l \in \mathbb{Z}^+$ is known and $\delta(k) \in \mathbb{R}$ is the time-varying part of $\tau(k)$ assumed to be unknown and bounded by $0 \leq \delta(k) < mT$, with $m \in \mathbb{Z}^+$ being also known.

In the next developments, the case when $m = 1$ is assumed. This means that the variation part of the delay is less than one sampling interval. Note that the theory can be easily extended for $m > 1$ by employing some steps presented in [294].

To proceed, let's assume that the fault $\boldsymbol{f}$ is constant during each sampling interval T, what is a reasonable assumption from a practical point of view[3], then the discrete representation of (3.7) and (3.8) is

$$\begin{cases} \boldsymbol{x}(k+1) = \bar{\boldsymbol{A}}\boldsymbol{x}(k) + \boldsymbol{\Gamma}_0(\delta(k))\boldsymbol{u}_c(k-l) + \boldsymbol{\Gamma}_1(\delta(k))\boldsymbol{u}_c(k-l-1) + \bar{\boldsymbol{E}}_f\boldsymbol{f}(k) \\ \quad \boldsymbol{y}(k) = \bar{\boldsymbol{C}}\boldsymbol{x}(k) \end{cases} \tag{3.12}$$

where

$$\begin{aligned} \bar{\boldsymbol{A}} &= e^{\boldsymbol{A}T}, \quad \boldsymbol{\Gamma}_0(\delta(k)) = \int_0^{T-\delta(k)} e^{\boldsymbol{A}t}dt\boldsymbol{B}, \quad \bar{\boldsymbol{E}}_f = \int_0^{T} e^{\boldsymbol{A}t}dt\boldsymbol{E}_f \\ \bar{\boldsymbol{C}} &= \boldsymbol{C}, \qquad \boldsymbol{\Gamma}_1(\delta(k)) = \int_{T-\delta(k)}^{T} e^{\boldsymbol{A}t}dt\boldsymbol{B} \end{aligned}$$

It is obvious that the following holds

$$\bar{\boldsymbol{B}} = \boldsymbol{\Gamma}_0(\delta(k)) + \boldsymbol{\Gamma}_1(\delta(k)) = \int_0^T e^{\boldsymbol{A}t}dt\boldsymbol{B} \tag{3.13}$$

Introducing a new augmented state vector $\boldsymbol{z}(k) = \begin{bmatrix}\boldsymbol{x}^T(k) & \boldsymbol{u}_c^T(k-l-1)\end{bmatrix}^T$ and using (3.13), (3.12) can be rewritten as

$$\begin{cases} \boldsymbol{z}(k+1) = \left(\hat{\boldsymbol{A}}_0 + \hat{\boldsymbol{A}}(\delta(k))\right)\boldsymbol{z}(k) + \left(\hat{\boldsymbol{B}}_0 + \hat{\boldsymbol{B}}(\delta(k))\right)\boldsymbol{u}_c(k-l) + \hat{\boldsymbol{E}}_f\boldsymbol{f}(k) \\ \quad \boldsymbol{y}(k) = \hat{\boldsymbol{C}}\boldsymbol{z}(k) \end{cases} \tag{3.14}$$

[2]Note that there exist frequency (norm) based approaches to tackle this problem in an approximative (decoupling) manner, see Section 1.3.4 of Chapter 1

[3]The counterpart of this assumption is that the sampling interval T is chosen adequately so that (3.12) holds.

where

$$\hat{\boldsymbol{A}}_0 = \begin{bmatrix} \bar{\boldsymbol{A}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix}, \quad \hat{\boldsymbol{A}}(\delta(k)) = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{\Gamma}_1(\delta(k)) \\ \boldsymbol{0} & \boldsymbol{0} \end{bmatrix}, \quad \hat{\boldsymbol{C}} = \begin{bmatrix} \bar{\boldsymbol{C}} & \boldsymbol{0} \end{bmatrix}$$
$$\hat{\boldsymbol{B}}_0 = \begin{bmatrix} \bar{\boldsymbol{B}} \\ \boldsymbol{I} \end{bmatrix}, \quad \hat{\boldsymbol{B}}(\delta(k)) = \begin{bmatrix} -\boldsymbol{\Gamma}_1(\delta(k)) \\ \boldsymbol{0} \end{bmatrix}, \quad \hat{\boldsymbol{E}}_f = \begin{bmatrix} \bar{\boldsymbol{E}}_f \\ \boldsymbol{0} \end{bmatrix}$$

The system (3.14) is an uncertain linear parameter-varying system, where $\boldsymbol{\Gamma}_1$ is strongly dependent on the uncertain parameter $\delta(k)$. The task is now to transform this system to an uncertain polytopic system for which structured properties can be extracted in terms of unknown inputs. The polytopic system is then rewritten as a LTI system subject to an unknown input with a suitable distribution matrix.

3.2.3.1 Uncertainty Transformation Using Cayley-Hamilton Theorem

The following proposition gives a way to transform the uncertainty $\boldsymbol{\Gamma}_1(\delta(k))$ as an convex polytope. (The index a outlines that the first, a-method is considered.)

Proposition 3.1. *The Cayley-Hamilton theorem based transformation of $\boldsymbol{\Gamma}_1(\delta(k))$ can be expressed as the convex matrix polytope*

$$\boldsymbol{\Gamma}_1^a(\delta(k)) = \sum_{i=1}^{2n_x} \mu_i^a(k)\boldsymbol{U}_i^a \tag{3.15}$$

where $\mu_i^a(k) > 0, i = 1, ..., 2n_x, \forall k \in \mathbb{Z}^+$ are uncertain scale factors satisfying $\sum_{i=1}^{2n_x} \mu_i^a(k) = 1, \forall k \in \mathbb{Z}^+$, and $\boldsymbol{U}_i^a, i = 1, \ldots, 2n_x$ are known constant matrices defined as

$$\boldsymbol{U}_{2i-1}^a = n_x s_i^{\min} \boldsymbol{A}^{i-1}\boldsymbol{B}, \quad \boldsymbol{U}_{2i}^a = n_x s_i^{\max} \boldsymbol{A}^{i-1}\boldsymbol{B} \tag{3.16}$$

with

$$s_i^{\max} = \max_{0 \le \delta(k) \le T} \int_{T-\delta(k)}^{T} s_i(t)dt, \quad i = 1, 2, \ldots, n_x \tag{3.17}$$

$$s_i^{\min} = \min_{0 \le \delta(k) \le T} \int_{T-\delta(k)}^{T} s_i(t)dt, \quad i = 1, 2, \ldots, n_x \tag{3.18}$$

where $s_i(t), i = 1, 2, \ldots, n_x$ are the solutions to the n_x-th order homogenous scalar differential equation

$$\frac{d^{n_x}s(t)}{dt^{n_x}} + c_{n_x-1}\frac{d^{n_x-1}s(t)}{dt^{n_x-1}} + \ldots + c_1\dot{s}(t) + c_0 s(t) = 0 \tag{3.19}$$

satisfying the following initial conditions

$$\frac{d^{i-1}s_i(0)}{dt^{i-1}} = 1, \quad \frac{d^j s_i(0)}{dt^j} = 0 \quad \textit{for} \quad j \neq i-1, 0 \le j \le n_x - 1$$

Proof. Consider first the Cayley-Hamilton theorem, according to which the characteristic polynomial of a matrix $\boldsymbol{A}$ can be expressed as follows

$$p(\lambda) = \det(\lambda\boldsymbol{I} - \boldsymbol{A}) = \lambda^{n_x} + c_{n-1}\lambda^{n_x-1} + \ldots + c_1\lambda + c_0 \tag{3.20}$$

then according to Leonard [174], $e^{\boldsymbol{A}t}$ can be written as

$$e^{\boldsymbol{A}t} = s_1(t)\boldsymbol{I} + s_2(t)\boldsymbol{A} + \ldots + s_{n_x}(t)\boldsymbol{A}^{n_x-1} \tag{3.21}$$

where $s_i(t), i = 1, 2, \ldots, n_x$ are solutions to (3.19). Using (3.21), it is possible to express $\boldsymbol{\Gamma}_1(\delta(k))$ as follows

$$\boldsymbol{\Gamma}_1^a(\delta(k)) = \int\limits_{T-\delta(k)}^{T} e^{\boldsymbol{A}t}dt\boldsymbol{B} = \sum_{i=1}^{n_x}\left[\left(\int\limits_{T-\delta(k)}^{T} s_i(t)dt\right)\boldsymbol{A}^{i-1}\boldsymbol{B}\right] \tag{3.22}$$

Considering (3.17) and (3.18), then (3.22) can be rewritten as

$$\boldsymbol{\Gamma}_1^a(\delta(k)) = \sum_{i=1}^{n_x}\left(\alpha_{i,0}(k)s_i^{\min} + \alpha_{i,1}(k)s_i^{\max}\right)\boldsymbol{A}^{i-1}\boldsymbol{B} \tag{3.23}$$

where $\alpha_{i,0}(k)$, $\alpha_{i,1}(k), i = 1, \ldots, n_x$ are two time-varying unknown parameters satisfying $0 \leq \alpha_{i,0}(k) \leq 1$, $0 \leq \alpha_{i,1}(k) \leq 1$, and $\alpha_{i,0}(k) + \alpha_{i,1}(k) = 1$ for $\forall k \in \mathbb{Z}^+$. It can be verified [294] that $\int_{T-\delta(k)}^{T} s_i(t)dt, i = 1, 2, \ldots, n_x$ are Lipschitz-continuous on $0 \leq \delta(k) \leq T$, i.e., they satisfy

$$\left|\int_{T-\delta_1(k)}^{T} s_i(t)dt - \int_{T-\delta_2(k)}^{T} s_i(t)dt\right| \leq \gamma_i\left|\delta_1(k) - \delta_2(k)\right|, \quad \forall\delta_1(k), \delta_2(k) \in [0, T]$$

where $\gamma_i, i = 1, 2, ..., n_x$ are the Lipschitz constants.

Considering (3.16) together with $\mu_{2i-1}^a(k) = \alpha_{i,0}(k)/n_x$ and $\mu_{2i}^a(k) = \alpha_{i,1}(k)/n_x$, it can be verified that (3.23) yields (3.15) and $\mu_i^a(k) > 0$, $\sum_{i=1}^{2n_x}\mu_i^a(k) = 1$ holds $\forall k \in \mathbb{Z}^+$. ■

Remark 3.2. *Note that the Lipschitz constants are not unique, they can be any finite constants satisfying the Lipschitz inequality. Therefore, according to [294], when s_i^{max} and s_i^{min} cannot be obtained analytically, reliable Lipschitz global optimization algorithms (e.g., Piyavskii's algorithm), which can guarantee a global convergence for all Lipschitz-continuous functions in a closed interval [241], can be adopted to find $s_i^{\max}$ and $s_i^{\min}$ no matter $s_i(t)$, $i = 1, 2, \ldots, n_x$ are convex or not.*

Remark 3.3. *From the derivation above, it can be concluded that the number of vertices of the polytopic representation is $2n_x$ (when considering $0 \leq \delta(k) \leq T$), which is a linear function of the system order.*

3.2.3.2 Uncertainty Transformation Using Taylor Series Expansion

The second transformation is based on the h-order Taylor series expansion [139] and is given the following proposition. (Here the index b denotes the second, b-method.)

Proposition 3.2. *The h-order Taylor series approximation of $\boldsymbol{\Gamma}_1(\delta(k))$ can be expressed as the convex matrix polytope*

$$\boldsymbol{\Gamma}_1^b(\delta(k)) \doteq \sum_{i=1}^{h+1}\mu_i^b(k)\boldsymbol{U}_i^b \tag{3.24}$$

where $\mu_i^b(k) > 0, i = 1, ..., h+1, \forall k \in \mathbb{Z}^+$ are uncertain scale factors satisfying $\sum\limits_{i=1}^{h+1}\mu_i^b(k) =$

$1, \forall k \in \mathbb{Z}^+$, *and* $\boldsymbol{U}_i^b, i = 1, \ldots, h+1$ *are known constant matrices, i.e.:*

$$\boldsymbol{U}_i^b = \left[\begin{array}{ccc} \boldsymbol{G}_h, & \ldots & , \boldsymbol{G}_1 \end{array} \right] \boldsymbol{\Phi}_i, \quad i = 1, \ldots, h+1 \tag{3.25}$$

with

$$\begin{aligned}
\boldsymbol{G}_i &= (-1)^{i+1} \frac{\boldsymbol{A}^{i-1}}{i!} e^{\mathbf{A}T} \boldsymbol{B}, \; i = 1, \ldots, h \\
\boldsymbol{\Phi}_1 &= \left[\begin{array}{ccccc} \delta_{min}^h \boldsymbol{I} & \delta_{min}^{h-1} \boldsymbol{I} & ,..., & \delta_{min}^2 \boldsymbol{I} & \delta_{min} \boldsymbol{I} \end{array} \right]^T \\
\boldsymbol{\Phi}_2 &= \left[\begin{array}{ccccc} \delta_{min}^h \boldsymbol{I} & \delta_{min}^{h-1} \boldsymbol{I} & ,..., & \delta_{min}^2 \boldsymbol{I} & \delta_{max} \boldsymbol{I} \end{array} \right]^T \\
&\vdots \\
\boldsymbol{\Phi}_{h+1} &= \left[\begin{array}{ccccc} \delta_{max}^h \boldsymbol{I} & \delta_{max}^{h-1} \boldsymbol{I} & ,..., & \delta_{max}^2 \boldsymbol{I} & \delta_{max} \boldsymbol{I} \end{array} \right]^T
\end{aligned}$$

Proof. Consider

$$\boldsymbol{F}(x) = \int_{T-x}^{T} e^{\boldsymbol{A}s} ds \tag{3.26}$$

then using the Taylor series expansion, one can write

$$\boldsymbol{F}(x) = \boldsymbol{F}(0) + \dot{\boldsymbol{F}}(0)x + \ddot{\boldsymbol{F}}(0)\frac{x^2}{2!} + \ldots + \frac{d^i \boldsymbol{F}}{dx^i}(0)\frac{x^i}{i!} + \ldots = -\sum_{i=1}^{\infty} \frac{(-x)^i}{i!} \boldsymbol{A}^{i-1} e^{\boldsymbol{A}T} \tag{3.27}$$

Taylor series expansion of the uncertainty $\boldsymbol{\Gamma}_1(\delta(k)) = \int_{T-\delta(k)}^{T} e^{\boldsymbol{A}t} dt \boldsymbol{B}$ can be obtained from (3.26) and (3.27) using $x = \delta(k)$ as follows

$$\boldsymbol{\Gamma}_1^b(\delta(k)) = -\sum_{i=1}^{\infty} (-\delta(k))^i \frac{\boldsymbol{A}^{i-1}}{i!} e^{\boldsymbol{A}T} \boldsymbol{B}$$

Then, the h-order approximation of the Taylor series expansion for the uncertainty $\boldsymbol{\Gamma}_1(\delta(k))$ can be expressed as a finite sum of the first h elements

$$\boldsymbol{\Gamma}_1^b(\delta(k)) \doteq -\sum_{i=1}^{h} (-\delta(k))^i \frac{\boldsymbol{A}^{i-1}}{i!} e^{\boldsymbol{A}T} \boldsymbol{B} \tag{3.28}$$

The approximation error is given by the remainder $\boldsymbol{\Xi}_h$, i.e.,

$$\boldsymbol{\Xi}_h = -\sum_{i=h+1}^{\infty} (-\delta(k))^i \frac{\boldsymbol{A}^{i-1}}{i!} e^{\boldsymbol{A}T} \boldsymbol{B} = \left(\sum_{i=1}^{h} (-\delta(k))^i \frac{\boldsymbol{A}^{i-1}}{i!} e^{\boldsymbol{A}T} - \int_{T}^{T-\delta(k)} e^{\boldsymbol{A}t} dt \right) \boldsymbol{B}$$

In [139], it was shown that if

$$\begin{aligned}
\mu_1^b(k) &= 1 - \frac{\delta(k) - \delta_{min}}{\delta_{max} - \delta_{min}}, \\
\mu_i^b(k) &= \frac{\delta^{i-1}(k) - \delta_{min}^{i-1}}{\delta_{max}^{i-1} - \delta_{min}^{i-1}} - \frac{\delta^i(k) - \delta_{min}^i}{\delta_{max}^i - \delta_{min}^i}, \quad i = 2, \ldots, h
\end{aligned} \tag{3.29}$$

where $\delta_{min} = \min\{\delta(k)\}$, $\delta_{max} = \max\{\delta(k)\}$, and thus $\delta(k) \in [\delta_{min}, \delta_{max}], \forall k \in \mathbb{Z}^+$, then $\mu_i^b(k) > 0, i = 1, ..., h+1$ and $\sum_{i=1}^{h+1} \mu_i^b(k) = 1, \forall k \in \mathbb{Z}^+$. Using (3.29), (3.28) and (3.25), the convex

matrix polytope (3.24), given in Proposition 3.2, yields. ■

3.2.4 Approximation of the Uncertainty in Terms of Unknown Inputs

Taking into account the structure of the uncertain matrices $\hat{\boldsymbol{A}}(\delta)$ and $\hat{\boldsymbol{B}}(\delta)$ in (3.14) and the two transformations of $\boldsymbol{\Gamma}_1(\delta)$ introduced in Proposition 3.1 and Proposition 3.2, the influence of the uncertain scalar factors μ_i^a and μ_i^b on the state $\boldsymbol{x}$ can be approximated in terms of unknown inputs as follows

$$\sum_{i=1}^{2n_x} \mu_i^a(k)\boldsymbol{U}_i^a\Big(\boldsymbol{u}_c(k-l-1)-\boldsymbol{u}_c(k-l)\Big) = \boldsymbol{E}_d^a\boldsymbol{d}_a(k) \tag{3.30}$$

$$\sum_{i=1}^{h+1} \mu_i^b(k)\boldsymbol{U}_i^b\Big(\boldsymbol{u}_c(k-l-1)-\boldsymbol{u}_c(k-l)\Big) = \boldsymbol{E}_d^b\boldsymbol{d}_b(k) \tag{3.31}$$

where

$$\boldsymbol{d}_a(k) = \Big[\mu_1^a(k)(\boldsymbol{u}_c^T(k-l-1)-\boldsymbol{u}_c^T(k-l)),\ldots,\mu_{2n_x}^a(k)(\boldsymbol{u}_c^T(k-l-1)-\boldsymbol{u}_c^T(k-l))\Big]^T$$

$$\boldsymbol{d}_b(k) = \Big[\mu_1^b(k)(\boldsymbol{u}_c^T(k-l-1)-\boldsymbol{u}_c^T(k-l)),\ldots,\mu_{h+1}^b(k)(\boldsymbol{u}_c^T(k-l-1)-\boldsymbol{u}_c^T(k-l))\Big]^T$$

$$\boldsymbol{E}_d^a = \left[\boldsymbol{U}_1^a,\ldots,\boldsymbol{U}_{2n_x}^a\right], \qquad \boldsymbol{E}_d^b = \Big[\boldsymbol{U}_1^b,\ldots,\boldsymbol{U}_{h+1}^b\Big]$$

These two distribution matrices, $\boldsymbol{E}_d^a$ and $\boldsymbol{E}_d^b$, aim to model the uncertainty-entry directions in two different ways. Therefore, in order to preserve all these directions, i.e., not use only a single approach, an augmented distribution matrix $\hat{\boldsymbol{E}}_d$ and an augmented unknown input $\boldsymbol{d}$ is considered so that

$$\hat{\boldsymbol{E}}_d = \begin{bmatrix}\bar{\boldsymbol{E}}_d\\ \boldsymbol{0}\end{bmatrix}, \quad \boldsymbol{d}(k) = \begin{bmatrix}\boldsymbol{d}_a(k)\\ \boldsymbol{d}_b(k)\end{bmatrix} \tag{3.32}$$

where $\bar{\boldsymbol{E}}_d = \Big[\boldsymbol{E}_d^a \quad \boldsymbol{E}_d^b\Big]$. The elements (columns) of $\hat{\boldsymbol{E}}_d$ define the directions how each component of $\boldsymbol{d}$ affects the augmented state $\boldsymbol{z}$. This kind of approach gains advantage of combining two techniques to model the effect of the complex uncertainty δ on the state.

Finally, the augmented model with lumped unknown inputs can be expressed as

$$\begin{cases} \boldsymbol{z}(k+1) = \hat{\boldsymbol{A}}_0\boldsymbol{z}_k + \hat{\boldsymbol{B}}_0\boldsymbol{u}_c(k-l) + \hat{\boldsymbol{E}}_f\boldsymbol{f}(k) + \hat{\boldsymbol{E}}_d\boldsymbol{d}(k) \\ \boldsymbol{y}(k) = \hat{\boldsymbol{C}}\boldsymbol{z}(k) \end{cases} \tag{3.33}$$

This model is a quasi-equivalent representation of the augmented system given in (3.14). In other words, using two polytopic transformations, the influence of the uncertainty $\boldsymbol{\Gamma}_1(\delta)$ (that models the effect of the unknown time-varying delays induced by the CPDE electronic device) on the augmented state $\boldsymbol{z}$ is approximated in terms of the unknown input $\boldsymbol{d}$.

By closer examining the structure of $\hat{\boldsymbol{A}}_0, \hat{\boldsymbol{B}}_0, \hat{\boldsymbol{E}}_f, \hat{\boldsymbol{E}}_d$ in (3.33), one can see that only the upper state of $\boldsymbol{z}$, i.e., the system state $\boldsymbol{x}$, is influenced by $\boldsymbol{f}$ and $\boldsymbol{d}$. It means that there is no coupling between the lower and upper state. This allows to consider only the upper state $\boldsymbol{x}$ in (3.33) for residual generator design.

3.2.5 Residual Generator Design with Decoupled Unknown Inputs

To solve Problem 3.1, the following observer-based residual generator is considered

$$\begin{cases} \hat{\boldsymbol{x}}(k+1) = (\bar{\boldsymbol{A}} - \bar{\boldsymbol{L}}\bar{\boldsymbol{C}})\hat{\boldsymbol{x}}(k) + \bar{\boldsymbol{B}}\boldsymbol{u}_c(k-l) + \bar{\boldsymbol{L}}\boldsymbol{y}(k) \\ \boldsymbol{r}(k) = \bar{\boldsymbol{Q}}(\boldsymbol{y}(k) - \bar{\boldsymbol{C}}\hat{\boldsymbol{x}}(k)) \end{cases} \tag{3.34}$$

where $\boldsymbol{r} \in \mathbb{R}^{n_r}$ is the residual signal, $\hat{\boldsymbol{x}} \in \mathbb{R}^{n_x}$ the estimation of the state vector $\boldsymbol{x}$, $\bar{\boldsymbol{L}} \in \mathbb{R}^{n_x \times n_y}$ the observer gain and $\bar{\boldsymbol{Q}} \in \mathbb{R}^{n_r \times n_y}$ the residual weighting matrix, respectively.

Remark 3.4. *The residual generator given in the observer-like form* (3.34) *can be easily transformed into a transfer function-like form* (3.10)*, i.e.,* $\boldsymbol{H}_u(z) = -\bar{\boldsymbol{Q}}\bar{\boldsymbol{C}}[z\boldsymbol{I} - (\bar{\boldsymbol{A}} - \bar{\boldsymbol{L}}\bar{\boldsymbol{C}})]^{-1}\bar{\boldsymbol{B}}$ *and* $\boldsymbol{H}_y(z) = \bar{\boldsymbol{Q}}\left[\boldsymbol{I} - \bar{\boldsymbol{C}}[z\boldsymbol{I} - (\bar{\boldsymbol{A}} - \bar{\boldsymbol{L}}\bar{\boldsymbol{C}})]^{-1}\bar{\boldsymbol{L}}\right]$.

The Z-transformed residual response to faults and unknown inputs is

$$\boldsymbol{r}(z) = \boldsymbol{G}_{rf}(z)\boldsymbol{f}(z) + \boldsymbol{G}_{rd}(z)\boldsymbol{d}(z) \tag{3.35}$$

where

$$\boldsymbol{G}_{rf}(z) = \bar{\boldsymbol{Q}}\bar{\boldsymbol{C}}(z\boldsymbol{I} - \bar{\boldsymbol{A}} + \bar{\boldsymbol{L}}\bar{\boldsymbol{C}})^{-1}\bar{\boldsymbol{E}}_f \tag{3.36}$$

$$\boldsymbol{G}_{rd}(z) = \bar{\boldsymbol{Q}}\bar{\boldsymbol{C}}(z\boldsymbol{I} - \bar{\boldsymbol{A}} + \bar{\boldsymbol{L}}\bar{\boldsymbol{C}})^{-1}\bar{\boldsymbol{E}}_d \tag{3.37}$$

In (3.35), $\boldsymbol{G}_{rf}(z)$ and $\boldsymbol{G}_{rd}(z)$ denote the transfers between $\boldsymbol{f}(z)$ and $\boldsymbol{r}(z)$, and $\boldsymbol{d}(z)$ and $\boldsymbol{r}(z)$, respectively.

Once $\bar{\boldsymbol{E}}_d$ is known, the remaining problem is to find matrices $\bar{\boldsymbol{L}}$ and $\bar{\boldsymbol{Q}}$ so that $(\bar{\boldsymbol{A}} - \bar{\boldsymbol{L}}\bar{\boldsymbol{C}})$ is stable, and $\boldsymbol{G}_{rd}(z) = \boldsymbol{0}$ holds. The assignment of the observer eigenvectors and eigenvalues is a direct way to solve this design problem. Additionally, the assignment of the eigenvalues enables to adequately manage the dynamics of the observer. Note that, because this technique does not consider a sensitivity constraint in the design procedure, the fault sensitivity performance of the proposed residual generator can only be verified a posteriori. Especially, the subspace of the considered faults should not intersect the subspace of decoupled disturbances, i.e., $\mathrm{Im}(\bar{\boldsymbol{E}}_f) \not\subset \mathrm{Im}(\bar{\boldsymbol{E}}_d)$ (separability condition). See the discussion in [61] if necessary.

To proceed, two lemmas which relate the eigenstructure properties of the system are introduced.

Lemma 3.1 (Chen and Patton [39])**.** *Any transfer function matrix (resolvent matrix) can be expanded in term of eigenstructure:*

$$(z\boldsymbol{I} - \bar{\boldsymbol{A}}_c)^{-1} = \frac{\boldsymbol{v}_1\boldsymbol{p}_1^T}{z - \lambda_1} + \frac{\boldsymbol{v}_2\boldsymbol{p}_2^T}{z - \lambda_2} + \ldots + \frac{\boldsymbol{v}_{n_x}\boldsymbol{p}_{n_x}^T}{z - \lambda_{n_x}} \tag{3.38}$$

where $\boldsymbol{v}_i$ *is the right and* $\boldsymbol{p}_i^T$ *is the left eigenvector of* $\bar{\boldsymbol{A}}_c = \bar{\boldsymbol{A}} - \bar{\boldsymbol{L}}\bar{\boldsymbol{C}}$*, both corresponding to eigenvalue* $\lambda_i \in \Lambda(\bar{\boldsymbol{A}}_c)$.

Lemma 3.2 (Patton and Frank [229], Chap.4)**.** *A given left eigenvector* $\boldsymbol{p}_i^T$ *corresponding to eigenvalue* λ_i *of* $\bar{\boldsymbol{A}}_c$ *is always orthogonal to the right eigenvectors* $\boldsymbol{v}_j$ *corresponding to the remaining* $(n_x - 1)$ *eigenvalues* λ_j *of* $\bar{\boldsymbol{A}}_c$*, where* $\lambda_i \neq \lambda_j$.

Remark 3.5. *Note that Lemma 3.1 is only valid for cases when all eigenvectors of* $\bar{\boldsymbol{A}}_c$ *are different, however this requirement does not impose any restriction on the residual generator*

design.

Based on Lemma 3.1, the transfer function $\boldsymbol{G}_{rd}(z)$ can be expanded in terms of the eigenstructure as

$$\boldsymbol{G}_{rd}(z) = \sum_{i=1}^{n_x} \frac{\boldsymbol{\Upsilon}_i}{z - \lambda_i} = \sum_{i=1}^{n_x} \frac{\bar{\boldsymbol{H}}\boldsymbol{v}_i\boldsymbol{p}_i^T\bar{\boldsymbol{E}}_d}{z - \lambda_i} \tag{3.39}$$

where $\bar{\boldsymbol{H}} = \bar{\boldsymbol{Q}}\bar{\boldsymbol{C}}$ and $\boldsymbol{\Upsilon}_i = \bar{\boldsymbol{H}}\boldsymbol{v}_i\boldsymbol{p}_i^T\bar{\boldsymbol{E}}_d$, $i = 1, \ldots, n_x$.

It is obvious that the unknown input decoupling is feasible if and only if

$$\bar{\boldsymbol{H}}\boldsymbol{v}_i\boldsymbol{p}_i^T\bar{\boldsymbol{E}}_d = \boldsymbol{0}, \qquad \forall\, i = 1, \ldots, n_x \tag{3.40}$$

Let's define the left $\bar{\boldsymbol{P}}$ and right $\bar{\boldsymbol{V}}$ eigenvector matrices of $\bar{\boldsymbol{A}}_c$ as

$$\bar{\boldsymbol{P}} = \begin{bmatrix} \boldsymbol{p}_1, & \boldsymbol{p}_2 & \ldots & \boldsymbol{p}_{n_x} \end{bmatrix}^T, \quad \bar{\boldsymbol{V}} = \begin{bmatrix} \boldsymbol{v}_1, & \boldsymbol{v}_2 & \ldots & \boldsymbol{v}_{n_x} \end{bmatrix} \tag{3.41}$$

Based on Lemma 3.2, the following relation holds

$$\bar{\boldsymbol{P}}\bar{\boldsymbol{V}} = \begin{bmatrix} \boldsymbol{p}_1^T\boldsymbol{v}_1 & 0 & \ldots & 0 \\ 0 & \boldsymbol{p}_2^T\boldsymbol{v}_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \boldsymbol{p}_{n_x}^T\boldsymbol{v}_{n_x} \end{bmatrix} \tag{3.42}$$

If vectors $\boldsymbol{p}_i^T$ and $\boldsymbol{v}_i$ $(i = 1, \ldots, n_x)$ are properly scaled, the above equation becomes

$$\bar{\boldsymbol{P}}\bar{\boldsymbol{V}} = \boldsymbol{I} \tag{3.43}$$

This also means that $\bar{\boldsymbol{P}} = \bar{\boldsymbol{V}}^{-1}$. Using this property, (3.40) implies

$$\bar{\boldsymbol{H}}\left(\sum_{i=1}^{n_x}\boldsymbol{v}_i\boldsymbol{p}_i^T\right)\bar{\boldsymbol{E}}_d = \bar{\boldsymbol{H}}\bar{\boldsymbol{V}}\bar{\boldsymbol{P}}\bar{\boldsymbol{E}}_d = \bar{\boldsymbol{H}}\bar{\boldsymbol{E}}_d = \boldsymbol{Q}\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d = \boldsymbol{0} \tag{3.44}$$

Hence, one of the necessary conditions for designing an unknown input decoupled residual is given by (3.44) and restated in the following theorem.

Theorem 3.1 ([225])**.** *If the necessary condition*

$$\bar{\boldsymbol{Q}}\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d = \bar{\boldsymbol{H}}\bar{\boldsymbol{E}}_d = \boldsymbol{0} \tag{3.45}$$

holds and all the rows of the matrix $\bar{\boldsymbol{H}}$ are left eigenvectors of $\bar{\boldsymbol{A}}_c$ corresponding to any n_r eigenvalues of $\bar{\boldsymbol{A}}_c$, then $\boldsymbol{G}_{rd}(z) = \boldsymbol{0}$ is satisfied.

Proof. If the rows of $\bar{\boldsymbol{H}}$ are the n_r left eigenvectors $(\boldsymbol{p}_i,\ i = 1, \ldots, n_r)$ of $\bar{\boldsymbol{A}}_c$, i.e.,

$$\bar{\boldsymbol{H}} = \begin{bmatrix} \boldsymbol{p}_1 & \boldsymbol{p}_2 & \ldots & \boldsymbol{p}_{n_r} \end{bmatrix}^T \tag{3.46}$$

then using Lemma 3.2 the following must hold

$$\bar{\boldsymbol{H}}\boldsymbol{v}_i = \boldsymbol{0}, \quad i = n_r + 1, \ldots, n_x$$

According to the necessary condition (3.45), the following must hold too

$$\boldsymbol{p}_i^T \bar{\boldsymbol{E}}_d = \boldsymbol{0}, \quad i = 1, \ldots, n_r$$

From Lemma 3.1 it can be shown that $\boldsymbol{\Upsilon}_i = \boldsymbol{0}, \forall i = 1, \ldots, n_x$ and thus $\boldsymbol{G}_{rd}(z) = \boldsymbol{0}$ ■

3.2.5.1 Left Eigenstructure Assignment

Unknown input decoupling design via EA is to assign left observer eigenvectors orthogonal to all the columns of $\bar{\boldsymbol{E}}_d$. Following Theorem 3.1, the first step for the design of the unknown input decoupled residual generator (3.34) is to compute the weighting matrix $\bar{\boldsymbol{Q}}$ such that (3.45) is satisfied. If $\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d = \boldsymbol{0}$, any weighting matrix can satisfy (3.45). A general solution is however given by

$$\bar{\boldsymbol{Q}} = \bar{\boldsymbol{Q}}_1 \left(\boldsymbol{I} - \bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d (\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d)^\dagger \right) \tag{3.47}$$

where $\bar{\boldsymbol{Q}}_1 \in \mathbb{R}^{n_r \times n_y}$ is an arbitrary design matrix and $(\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d)^\dagger$ is the pseudoinverse of $(\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d)$ given in Appendix A.3.1. The maximum row rank of $\bar{\boldsymbol{Q}}$ is $n_y - \text{rank}(\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d)$, thus the residual signal dimension should be chosen according to

$$n_r \leq n_y - \text{rank}(\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d) \tag{3.48}$$

since the linearly dependent rows do not provide any useful information for fault diagnosis.

Remark 3.6. *For most cases, the rank condition* (3.48) *is not satisfied [39]. This condition also implies that if the number of independent columns $\bar{\boldsymbol{E}}_d$ is larger than the independent row number of $\bar{\boldsymbol{C}}$, i.e., the number of independent unknown inputs that should be decoupled is larger than the number of independent measurements, then an approximate decoupling procedure should be used (i.e., $\bar{\boldsymbol{E}}_d$ should be approximated by a lower-rank matrix), see e.g., [107].*

The second step is to determine the eigenstructure of the observer. All rows of $\bar{\boldsymbol{H}}$ must be the n_r left eigenvectors of $\bar{\boldsymbol{A}}_c$. For the given (stable) eigenvalue spectrum $\Lambda(\bar{\boldsymbol{A}}_c) = \{\lambda_i, i = 1, \ldots, n_x\}$, the following relation holds

$$\boldsymbol{p}_i^T (\lambda_i \boldsymbol{I} - \bar{\boldsymbol{A}}) = -\boldsymbol{p}_i^T \bar{\boldsymbol{L}}\bar{\boldsymbol{C}} = -\boldsymbol{m}_i^T \bar{\boldsymbol{C}}, \quad i = 1, \ldots, n_x \tag{3.49}$$

where $\boldsymbol{m}_i^T = \boldsymbol{p}_i^T \bar{\boldsymbol{L}}$. The assignability condition says that for each λ_i, the corresponding left eigenvector $\boldsymbol{p}_i^T$ should lie in the column subspace spanned by $\{\bar{\boldsymbol{C}}(\lambda_i \boldsymbol{I} - \bar{\boldsymbol{A}})^{-1}\}$, i.e., a vector $\boldsymbol{m}_i^T$ exists such that

$$\boldsymbol{p}_i^T = \boldsymbol{m}_i^T \bar{\boldsymbol{K}}_i, \qquad i = 1, \ldots, n_r \tag{3.50}$$

where $\bar{\boldsymbol{K}}_i = -\bar{\boldsymbol{C}}(\lambda_i \boldsymbol{I} - \bar{\boldsymbol{A}})^{-1}$, $i = 1, \ldots, n_r$. The projection of $\boldsymbol{p}_i$ in the subspace span$\{\bar{\boldsymbol{K}}_i\}$ is denoted by

$$\boldsymbol{p}_i^{\circ T} = \boldsymbol{m}_i^{\circ T} \bar{\boldsymbol{K}}_i, \qquad i = 1, \ldots, n_r \tag{3.51}$$

where $\boldsymbol{m}_i^{\circ T} = \boldsymbol{p}_i^T \bar{\boldsymbol{K}}_i^T (\bar{\boldsymbol{K}}_i \bar{\boldsymbol{K}}_i^T)^{-1}$, $i = 1, \ldots, n_r$.

If $\boldsymbol{p}_i^T = \boldsymbol{p}_i^{\circ T}$, then $\boldsymbol{p}_i^T$ is in span$\{\bar{\boldsymbol{K}}_i\}$, the required observer eigenstructure is assignable and perfect decoupling can be achieved. Otherwise, the eigenvectors must be chosen to be close, e.g., in a least-square sense $\|\boldsymbol{p}_i^T - \boldsymbol{p}_i^{\circ T}\|$, to the desired eigenvectors, i.e., an approximative procedure must be considered in order to replace $\boldsymbol{p}_i^T$ by its projection $\boldsymbol{p}_i^{\circ T}$. In this situation, the

residual is not perfectly decoupled, but has low sensitivity to unknown inputs due to approximate decoupling [222].

The remaining $n_x - n_r$ eigenvalues $(\lambda_i, i = n_r + 1, \ldots, n_x)$ and the corresponding eigenvectors $(\boldsymbol{p}_i^T, i = n_r + 1, \ldots, n_x)$ can be chosen freely from the assignable subspace, e.g., using Singular Value Decomposition (SVD). Finally, the observer matrix $\bar{\boldsymbol{L}}$ can be computed as follows

$$\bar{\boldsymbol{L}} = (\boldsymbol{P}^\sharp)^{-1}\boldsymbol{M}^\sharp \tag{3.52}$$

where

$$\boldsymbol{M}^\sharp = \begin{bmatrix} \boldsymbol{m}_1^\circ & \ldots & \boldsymbol{m}_{n_r}^\circ & \boldsymbol{m}_{n_{r+1}} & \ldots & \boldsymbol{m}_{n_x} \end{bmatrix}^T$$
$$\boldsymbol{P}^\sharp = \begin{bmatrix} \boldsymbol{p}_1^\circ & \ldots & \boldsymbol{p}_{n_r}^\circ & \boldsymbol{p}_{n_{r+1}} & \ldots & \boldsymbol{p}_{n_x} \end{bmatrix}^T$$

It is obvious that, the first n_r eigenvalues corresponding to the required eigenvectors $\boldsymbol{p}_i^T, i = 1, \ldots, n_r$ must be real because all these eigenvectors are real-valued.

Remark 3.7. *There is no loss of generality in assuming that $\bar{\boldsymbol{E}}_d$ has a full column rank. When this is not the case, the following decomposition can be applied: $\bar{\boldsymbol{E}}_d\boldsymbol{d} = \bar{\boldsymbol{E}}_{d1}\bar{\boldsymbol{E}}_{d2}\boldsymbol{d}$, where $\bar{\boldsymbol{E}}_{d1}$ is a full column rank matrix and $\boldsymbol{d}_1 = \bar{\boldsymbol{E}}_{d2}\boldsymbol{d}$ can be considered as a new unknown input (see, e.g., [39]).*

3.2.6 Computational Procedure and Comments on Implementation Issues

First, the position model (3.3) and the attitude model (3.4) are transformed into the discrete form (3.12) with $T = 0.1$ s, $l = 0$ and $m = 1$. Practically it means that the unknown time-varying delay $\tau(k)$ is assumed to be in the closed interval $[0, T)$. Using the Cayley-Hamilton theorem-based transformation (given in Proposition 3.1) and the 2nd-order ($h = 2$) Taylor series expansion-based approximation (given in Proposition 3.2), the uncertainty $\boldsymbol{\Gamma}_1(\delta(k))$ is transformed into an unknown input as in (3.32).

The resulting matrix $\bar{\boldsymbol{E}}_d$ has a large number of columns and the rank condition given by (3.48) cannot be explicitly satisfied, see also Remark 3.6. Hence, choosing the desired residual dimension equal to one, i.e., $n_r = 1$, the following low rank factorization is performed for both models:

$$\bar{\boldsymbol{E}}_d^* = \arg\min \|\bar{\boldsymbol{E}}_d - \bar{\boldsymbol{E}}_d^*\|_F^2, \quad \text{s.t.} \quad n_r = n_y - \text{rank}(\bar{\boldsymbol{C}}\bar{\boldsymbol{E}}_d^*) \tag{3.53}$$

By this factorization, the most significant directions are kept. Equation (3.53) is easy to solve using Singular Value Decomposition (SVD) of $\bar{\boldsymbol{E}}_d$ as follows [181]:

$$\bar{\boldsymbol{E}}_d = \bar{\boldsymbol{U}}_s\bar{\boldsymbol{S}}_s\bar{\boldsymbol{V}}_s^T \tag{3.54}$$

where $\bar{\boldsymbol{S}}_s = [\text{diag}(\sigma_1, \ldots, \sigma_{n_x}), \ \boldsymbol{0}]$, $\sigma_1 \leq \sigma_2 \leq \ldots \leq \sigma_{n_x}$ are the singular values of $\bar{\boldsymbol{E}}_d$, and $\bar{\boldsymbol{U}}_s$, $\bar{\boldsymbol{V}}_s$ are orthogonal matrices. Matrix $\bar{\boldsymbol{E}}_d^*$ which solves the constrained optimization problem (3.53) is given by [181]

$$\bar{\boldsymbol{E}}_d^* = \bar{\boldsymbol{U}}_s \left[\text{diag}(0, \ldots, 0, \sigma_{n_{r+1}}, \ldots \sigma_{n_x})\right] \bar{\boldsymbol{V}}_s^T \tag{3.55}$$

Finally, following Remark 3.7, a full column rank decomposition is performed on $\bar{\boldsymbol{E}}_d^*$ using again the SVD technique.

The obtained distribution matrix $\bar{\boldsymbol{E}}_d$ is then used for the residual generator (3.34) design. The left eigenvectors of the observer are assigned to be the rows of the matrix $\bar{\boldsymbol{H}} = \bar{\boldsymbol{Q}}\bar{\boldsymbol{C}}$, where the weighting $\bar{\boldsymbol{Q}}$ is determined such that (3.45) holds. In order to be able to compare the performances of both FDI schemes (first based on the position and the second based on the attitude model), the assigned stable eigenvalues, which determine the observer dynamics, are selected to be exactly the same for both models, i.e., $\Lambda(\bar{\boldsymbol{A}}_c) = \{0.85, 0.87, 0.89, 0.91, 0.93, 0.95\}$.

In order to avoid using an optimization procedure to determine s_i^{max} and s_i^{min} in (3.22), the solutions $s_i(t), i = 1, \ldots, n_x$ of the differential equation (3.19) are found numerically, and therefore, s_i^{max} and s_i^{min} can be found using a simple iterative method.

Remark 3.8. *It is worth noting that other exact unknown input (disturbance) decoupling methods exist, see for instance the book of Chen and Patton [39]. In our particular case only the left EA technique appeared to be a viable candidate. Other methods, such as UIO or right EA technique, violated some necessary conditions of the solution existence.*

3.2.7 Residual Evaluation - Fault Detection

Once the residual generation problem is solved, the problem is to make a decision about the fault presence. The GLR test is used here to detect changes in the residual statistical properties. The decision is made based on two hypotheses: the null hypothesis (H_0) means no fault is present, while the alternative hypothesis (H_1) indicates some anomaly in the system considered due to the thruster fault. In this case, the decision test $\varrho^{J_{th}}$ is defined according to

$$\varrho^{J_{th}}(k) = \begin{cases} 1, & S^{N_d}(k) > J_{th} \;\Rightarrow\; H_1 \text{ is accepted} \\ 0, & S^{N_d}(k) \leq J_{th} \;\Rightarrow\; H_0 \text{ is accepted} \end{cases} \tag{3.56}$$

where J_{th} is a fixed threshold selected by the designer and $S^{N_d}(k)$ is the GLR algorithm for the variance, see (B.50) and (B.53) in Appendix B. A higher value of J_{th} will obviously increase the non-detection rate while a lower threshold will increase the false alarm rate. The optimal value of J_{th} can be selected through Monte Carlo simulation. This approach is widely used in the FDI community to analyze the efficiency and performance of the designed algorithm [232]. The interested reader can refer to the monograph of Basseville and Nikiforov [10] for details on the threshold determination.

The following developments propose a solution to this problem. An isolation strategy is developed to uniquely isolate the faulty thruster. Moreover, it should be recalled that simultaneous faults are not considered here.

3.2.8 Residual Evaluation - Fault Isolation

As it has been already noted, in the considered thruster configuration, each thruster has its partner which provides the same torque directions but force in exactly opposite direction, see Fig. 3.3 for illustration. Therefore, a residual subspace approach (see Section 1.3.6) cannot guarantee a full coverage of the considered isolation problematic [190], because this approach cannot distinguish between faults in either thruster, but only in the thruster pair[4]. The same can

[4]However, this claim is valid only if the same initial design conditions are considered as stated in this chapter, i.e., when only a single 3DOF model (either position or attitude) is considered for fault diagnosis instead of a full

be concluded for the so-called "structured observer schemes" (see Section 1.3.6) which are based on making each residual signal sensitive to a subset of faults while being insensitive to another subset [93]. Moreover, this strategy requires a bank of observers to be designed and run in parallel, and thus, can pose some constraints on the on-board computational equipment.

3.2.8.1 Proposed Isolation Strategy

The proposed isolation strategy requires only one observer to be designed and run. It relies on a minimum $\underline{\sigma}_j^{N_s}$ or maximum $\bar{\sigma}_j^{N_s}$ cross-correlation criterion between the jth residual signal r_j (a general case when $n_r > 1$ is considered here) and the associated controlled thruster open durations $\tilde{u}_i, i \in \mathcal{S}_{all}$, i.e.,

$$\sigma_j^{N_s}(k) = \begin{cases} \underline{\sigma}_j^{N_s}(k) & \textbf{if} \text{ open-type thruster fault} \\ \bar{\sigma}_j^{N_s}(k) & \textbf{if} \text{ closed-type thruster fault} \end{cases} \tag{3.57}$$

where

$$\bar{\sigma}_j^{N_s}(k) = \underset{\forall i \in \mathcal{S}_{all}}{\arg\max} \left| \frac{1}{N_s+1} \sum_{l=k-N_s+1}^{k} r_j(l)\tilde{u}_i(l) \right|, \quad j \in \{1,\ldots,n_r\},\ \forall k \in \mathbb{Z}^+ \tag{3.58}$$

$$\underline{\sigma}_j^{N_s}(k) = \underset{\forall i \in \mathcal{S}_{all}}{\arg\min} \left| \frac{1}{N_s + \varpi_i^{N_s}(k)} \sum_{l=k-N_s+1}^{k} r_j(l)\tilde{u}_i(l) \right|, \quad j \in \{1,\ldots,n_r\},\ \forall k \in \mathbb{Z}^+ \tag{3.59}$$

with

$$\varpi_i^{N_s}(k) = 1 - \sum_{l=k-N_s+1}^{k} \phi_i(l), \quad \text{where} \quad \phi_i(l) = \begin{cases} 0 & \textbf{if} \quad \tilde{u}_i(l) \neq 0 \\ 1 & \textbf{if} \quad \tilde{u}_i(l) = 0 \end{cases}, \quad i = 1,\ldots,N$$

These cross-correlation functions are statistical quantities that try to find the associated thruster index that has the smallest/greatest impact on the resulting residual signal. For real-time reason, these criteria are computed on a N_s-length sliding-window. An increase in the value of N_s results in an elongated isolation delay. An optimal value of N_s has to be selected and it can be done through a MC campaign. The resulting index $\sigma_j^{N_s}(k) \in \{1,2,\ldots,N\}$ refers to the identified faulty thruster using the jth residual signal at time instance k.

Note that if the ith thruster is not used by the TMF, i.e., $\tilde{u}_i = 0$, the minimum cross-correlation function will possibly result in $\underline{\sigma}(k) = i$. This fact is taken into account by introducing the penalty function $\varpi_i^{N_s}(k)$ in (3.59). Furthermore, if the TMF does not consider the MIB constraint, then this fact should be incorporated in the penalty function $\varpi_i^{N_s}(k)$ as follows: $\phi_i(l) = 1$ if $\tilde{u}_i(l) \leq MIB, \forall i \in \mathcal{S}_{all}$.

Considering the residual dimension being $n_r > 1$, then one of the following three approaches can be used to determine a unique $\sigma^{N_s}(k)$, i.e.,

1) take the smallest/greatest cross-correlation among all the residuals;

2) use only one residual signal r_j, $j \in \{1,\ldots,n_r\}$, e.g., the first one $\sigma^{N_s} = \sigma_1^{N_s}$;

6DOF model.

3) using a "voting" scheme where, for each residual entry r_j a $\sigma_j^{N_s}$ is computed separately, and a "majority voting rule" is implemented, i.e., the resulting index by the most $\sigma_j^{N_s}$, $j = 1, \ldots, n_r$ is the identified faulty thruster.

Finally, the resulting thruster index is confirmed at time instant $t_i = kT$, if the following holds

$$\sigma^{N_s}(k) = \sigma^{N_s}(k-1) = \ldots = \sigma^{N_s}(k - N_c + 1) \tag{3.60}$$

where a confirmation window of length $N_c > 1$ is introduced in order to avoid initial transition phenomena. It also allows to increase the robustness property of the proposed FDI scheme.

Algorithm 1 Thruster Fault Detection and Isolation Algorithm

```
if ϱ^{J_th}(k_d) = 1 then
    Decision = Declare the fault presence at time t_d = k_d T;
    Start collecting the isolation signals σ^{N_s}(k), k ≥ k_d;
    if For a given N_c, (3.60) holds at time t_i = k_i T then
        Decision = Declare the i = σ^{N_s}(k_i)-th thruster to be faulty;
    end if
end if
```

A key feature of this isolation strategy is that it is static, and thus it has a low computational burden. The whole fault detection and isolation strategy is summarized in Algorithm 1

Remark 3.9. *It should be noted that an event resolution algorithm must be implemented for the decision given in* (3.61)*, since it is required to distinguish the fault cases 1-3 (open-type fault) from the case 2-4 (closed-type fault). Fortunately, because cases 1-3 imply a propellant overconsumption and since the chaser is equipped with a set of dedicated sensors (tank pressure and tank temperature sensors) that can be used to monitor the overall propellant consumption $\mathcal{P}$, this problem can be easily solved as follows: using the reading from these sensors and combining some laws of fluid mechanics, a "measurement-based estimate" $\hat{\mathcal{P}}_m$ of the actual fuel consumption can be computed. On the other hand, using the knowledge of the thrusters Specific Impulse (ISP) and the available (on-board) thruster firing times $\tilde{\boldsymbol{u}}$, another "firing-times-based estimate" $\hat{\mathcal{P}}_f$ can be established. Comparing these two quantities, the following event resolution logic is suggested*

$$\sigma_j^{N_s}(k) = \begin{cases} \underline{\sigma}_j^{N_s}(k) & \textbf{if} \quad \hat{\mathcal{P}}_m \geq \hat{\mathcal{P}}_f \\ \bar{\sigma}_j^{N_s}(k) & \textbf{if} \quad \hat{\mathcal{P}}_m < \hat{\mathcal{P}}_f \end{cases} \tag{3.61}$$

Another solution is to apply an additional, second threshold on the likelihood estimate $S^{N_d}(k)$ or directly to the norm of the residual signal $\|\boldsymbol{r}(k)\|$.

3.2.9 Tuning of the FDI Scheme

In order to ensure robustness, whilst being sensitive to faults, the threshold J_{th} has to be selected carefully. As suggested in Section 3.2.7, the optimal value of J_{th} can be selected through MC simulation. Here, a set of 200 fault-free closed-loop MC simulations was performed using a GLR sliding window of 10 samples, i.e., $N_d = 10$. In the following, the notation S^{10} is used to denote the considered GLR test. Figure 3.7 illustrates the obtained results of the MC analysis. It can

be clearly seen from this figure that, for both models, the GLR signal $S^{10}(k)$ is very unlikely to exceed the value 20 during the whole length of the simulation[5]. Therefore, a threshold $J_{th} = 20$ is chosen to ensure (ideally) a zero false alarm rate. For the isolation function $\sigma_j^{N_s}$ given by (3.61), a sliding window of $N_s = 10$ and a confirmation window of $N_c = 15$ samples is considered. Note that the residual dimension is $n_r = 1$, thus the index j is omitted for $\sigma_j^{N_s}$ in the following.

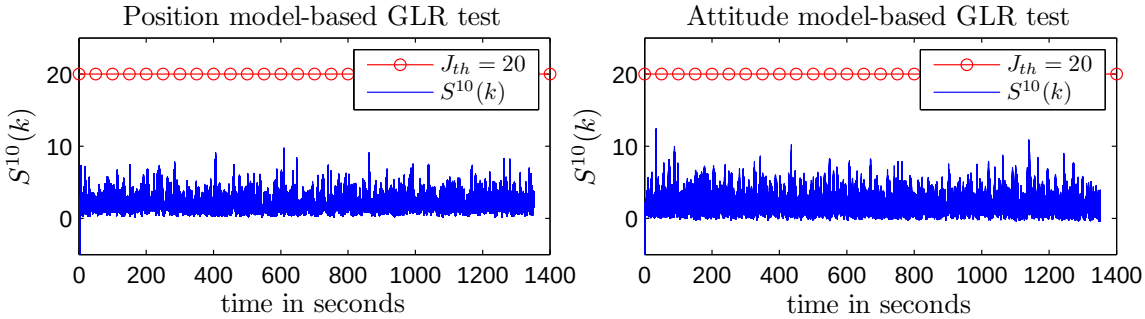


Figure 3.7 – GLR signals based on a set of 200 Monte Carlo simulations for fault-free case

3.3 Simulation Results

The two FDI schemes described in the previous section are next implemented within the MSR simulator to detect and a isolate single thruster fault affecting the chaser thruster-based propulsion system. The first scheme is based on the position model and the second on the attitude model one, respectively. Carefully selected robustness and FDI performance indices together with the Monte Carlo simulation campaign allow one to compare these schemes among each other.

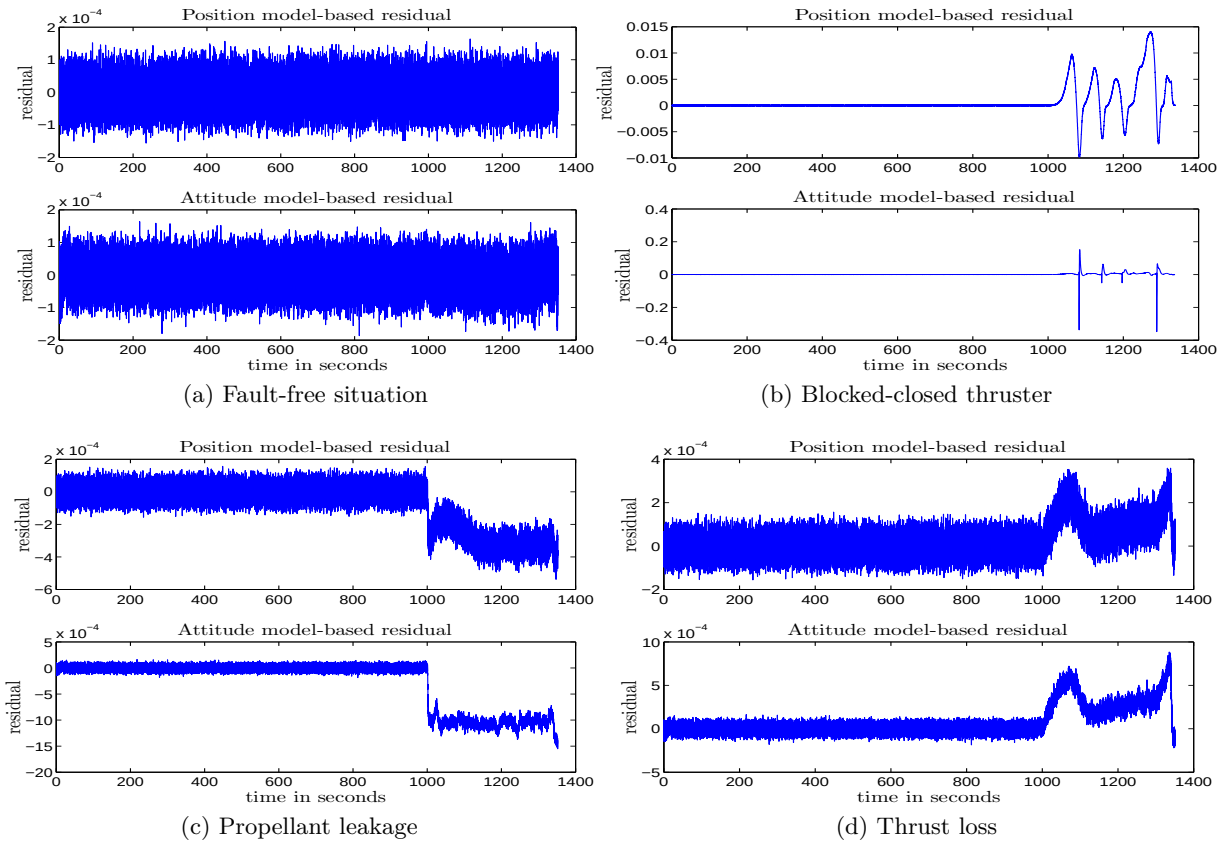
3.3.1 Residual Behaviour

In order to provide a qualitative analysis of the position model-based and attitude model-based residual behaviour, a comparison of four different scenarios is shown in Fig. 3.8. This figure illustrates the time behaviour of the residual signal, both in fault-free and faulty cases.

Fig. 3.8a corresponds to a fault-free situation. It can be observed that both residuals are very similar in terms of their variances. This allowed to select very similar parameters for the GLR test, i.e., for the parameters μ and σ_0 (see Appendix B.2.1.2). It also justifies why the selected threshold $J_{th} = 20$ resulted to be the same for both model-based schemes, see Section 3.2.9 for details.

Three other simulations have been performed in order to compare the fault-free residual with faulty cases. Fig. 3.8b corresponds to a blocked-closed thruster fault affecting thruster No.5. from $t_f = 1000s$. The rest two figures, i.e., Fig. 3.8c and Fig. 3.8d, correspond to a leaking thruster of size 10% and a loss of efficiency by 40%, respectively. In all the three cases,

[5]One can attach a certain false alarm probability (P_f) to the selected threshold J_{th} from the Cumulative Distribution Function (CDF) of the GLR test statistic plotted in Fig. 3.7. For example in [118], based on real flight data of an Unmanned Aerial Vehicle (UAV), the CDF of the GLR test statistics was found to be best fitted using a Weibull distribution. Using the fitted distribution, the detector threshold linked with a certain P_f was determined by looking at the right tail distribution to find the probability of exceeding a chosen threshold.



(a) Fault-free situation

(b) Blocked-closed thruster

(c) Propellant leakage

(d) Thrust loss

Figure 3.8 – Position and attitude model-based residual behaviours for different scenarios

thruster No.5 is considered to be faulty. All faults are maintained during the whole length of the simulation and are not accommodated (recovered).

In these particular cases, the blocked-closed thruster fault has the greatest impact on the residual behaviour (in terms of total magnitude), however the effect when this fault influences the residual is slightly later as it is in the later cases. As explained earlier, this can be due to the fact that an uncommanded thruster, which is deemed to be stuck-closed, has no effect on the spacecraft dynamics.

Figure 3.8c and Fig. 3.8d show that these fault types (leakage and thrust loss) have exactly opposite effect on the spacecraft dynamics, both in terms of rotational and translational dynamics since the residual behaves in opposite directions. A fully open thruster fault is not considered here. It is obvious that due to the direct link between the fully open thruster fault and a leakage type fault, i.e., without loss of generality a fully open thruster can be understood as a leakage fault with size 100%, the residual would have a very similar behaviour as the one depicted in Fig. 3.8c but obviously with much greater magnitude.

3.3.2 Monte Carlo Campaign

A Monte Carlo simulation campaign is used to test and validate the performance of the proposed FDI schemes when applied on a huge number of simulation models with randomly drawn dynamics. All considered simulations are carried out under realistic conditions except the event

resolution algorithm introduced in Remark 3.9, which is considered to work perfectly. For each run, model parameters, e.g., mass, CoM, inertia, etc. are altered within a specific limit, see Table 2.3 in Section 2.2.3. Navigation imperfections, spatial disturbances, time-varying delays induced by the CPDE electronic device and uncertainties on thruster rise times are also considered, see Chapter 2 for more details.

All together, a set of four $n_{mc} = 1600$ Monte Carlo simulations for each faulty case ($4 \times n_{mc}$) has been performed in order to assess the performance of the proposed FDI schemes. These fault scenarios correspond to:

- **Case 1:** fully open thruster ($m_{leak}(t) = 1, \forall t \geq t_f$)
- **Case 2:** blocked-closed thruster ($m_{leak}(t) = 1, \forall t \geq t_f$)
- **Case 3:** residual leakage ranging from 10% to 30% ($\hat{m}_{leak} \sim \mathcal{U}(0.1, 0.3)$, $m_s = 0.1$)
- **Case 4:** loss of efficiency ranging from 40% to 90% ($\hat{m}_{loss} \sim \mathcal{U}(0.4, 0.9)$)

Thruster faults have been uniformly distributed among all the 8 thrusters, see Fig. 3.11a for thruster indices distribution for all considered fault cases separately. Correspondingly, the leakage and the thrust loss size have been drawn from the uniform distribution with the following intervals: $\hat{m}_{leak} \in [10\%, 30\%]$ and $\hat{m}_{loss} \in [40\%, 90\%]$. The leakage is implemented as a dynamic lower saturation to the commanded thruster open rate, where this saturation starts at value 0 and ends at $\hat{m}_{leak}$ with a slope of $m_s = 0.1$, see Section 2.3.3 about fault modelling. In all cases, fault occurs at time $t_f = 1000$ s. Note that in this section, the recovery aspects are not considered, i.e., the fault remains present in the system during the whole length of the simulation and is not recovered.

Figures 3.9 and 3.10 illustrate the behaviour of the most important characteristics of the FDI units and their internal signals. Both the position model-based (left figures on Fig. 3.9 and 3.10) and attitude model-based (right figures on Fig. 3.9 and 3.10) FDI units are considered. These characteristics are:

i) the GLR signal $S^{10}(k)$ represented at each sample k and for a detection sliding window of length $N_d = 10$ samples, see (B.53);

ii) the decision (alarm) signal $\varrho^{20}(k)$ with the defined threshold $J_{th} = 20$, see (3.56);

iii) the thruster declared to be faulty by an isolation unit which is represented by the signal $\sigma^{10}(k)$ for a computation sliding window of length $N_s = 10$ samples, see (3.61)-(3.59).

The confirmation time window of length $N_c = 15$ samples is also considered. Figures 3.9 and 3.10 illustrate (from top to bottom) the above listed characteristics for the following set of four arbitrary chosen faulty scenarios from the MC campaign:

1. A fault that corresponds to a stuck open valve, occurring in the thruster No.8., i.e., the thruster No. 8 is fully opened so that it provides a maximum thrust.
2. A fully blocked-closed fault occurs in thruster No.3. In this case, the thruster does not generate any thrust regardless of the command by the TMF.
3. The third faulty situation corresponds to thruster No.2 suffering from a leakage with a final magnitude of 19.2%.

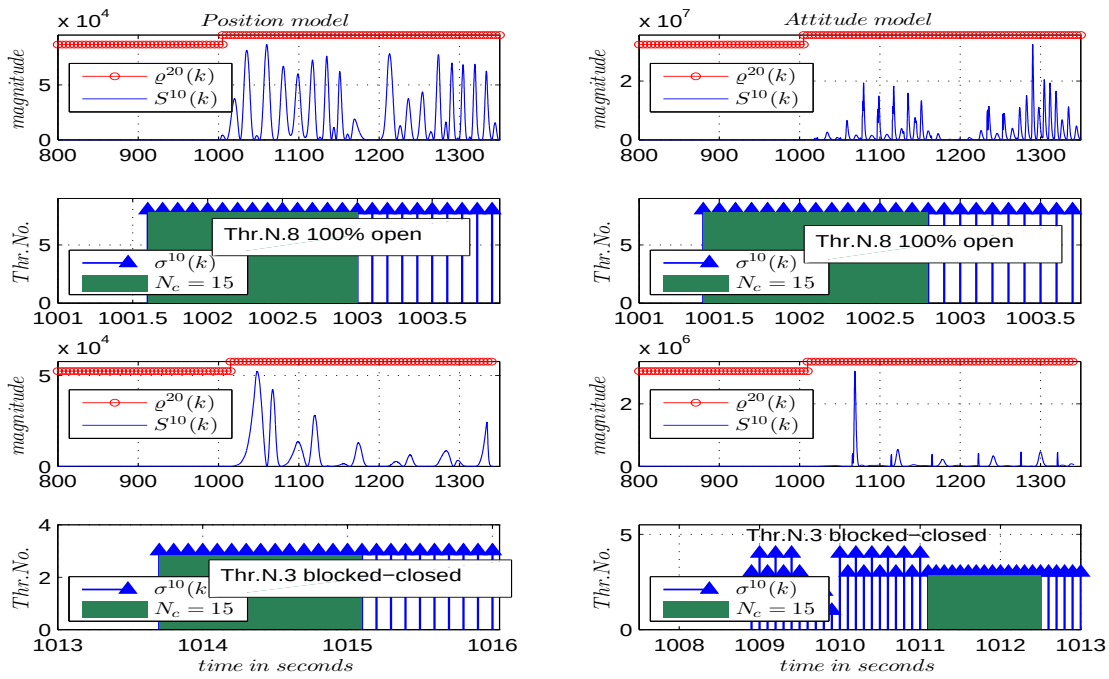


Figure 3.9 – Behaviour of the internal signals of the position (on the left) and attitude (on the right) model-based FDI scheme, respectively

4. The fourth faulty situation corresponds to the case when the thruster No.7 loses its thrust level by a value of 54.7%.

Figure 3.9 is concerned with the two first situations whereas Fig. 3.10 considers the two last cases. Clearly, the nonlinear simulations show that faults are detected and isolated by the proposed FDI units within a reasonable time. Moreover, Fig. 3.10 shows the ability to detect and isolate small (thrust loss) and incipient (residual leakage) thruster faults.

To evaluate and compare the performance and reliability of the two proposed FDI schemes, some statistical indices are computed. These indices are evaluated for the detection delay τ_d (time from fault occurrence to fault detection) and isolation delay τ_i (time from fault occurrence to fault isolation). The considered performance indices are listed below:

- $mean(\tau_d)/mean(\tau_i)$ - mean detection/isolation time,
- $std(\tau_d)/std(\tau_i)$ - standard deviation of the detection/isolation,
- p_i - true isolation rate (number of correctly isolated thrusters divided by n_{mc}),
- p_f - false alarm rate (number of wrongly detected faults divided by n_{mc}),
- p_{nd} - non-detection rate (number of non-detections divided by n_{mc}).

These performance indices are calculated for each fault scenario and model separately. Table 3.1 presents complete results obtained from the Monte Carlo simulation campaign. As it can be seen from this table, the two proposed FDI schemes present good reliability characteristics since no false alarms $p_f = 0$ and non-detections $p_{nd} = 0$ have been revealed. Furthermore, all thruster faults were correctly isolated at the end of the campaign (i.e., $p_i = 1$). These achieved results also demonstrate that each FDI scheme is able to successfully detect and isolate thruster faults affecting the chaser baseline thruster-based propulsion system.

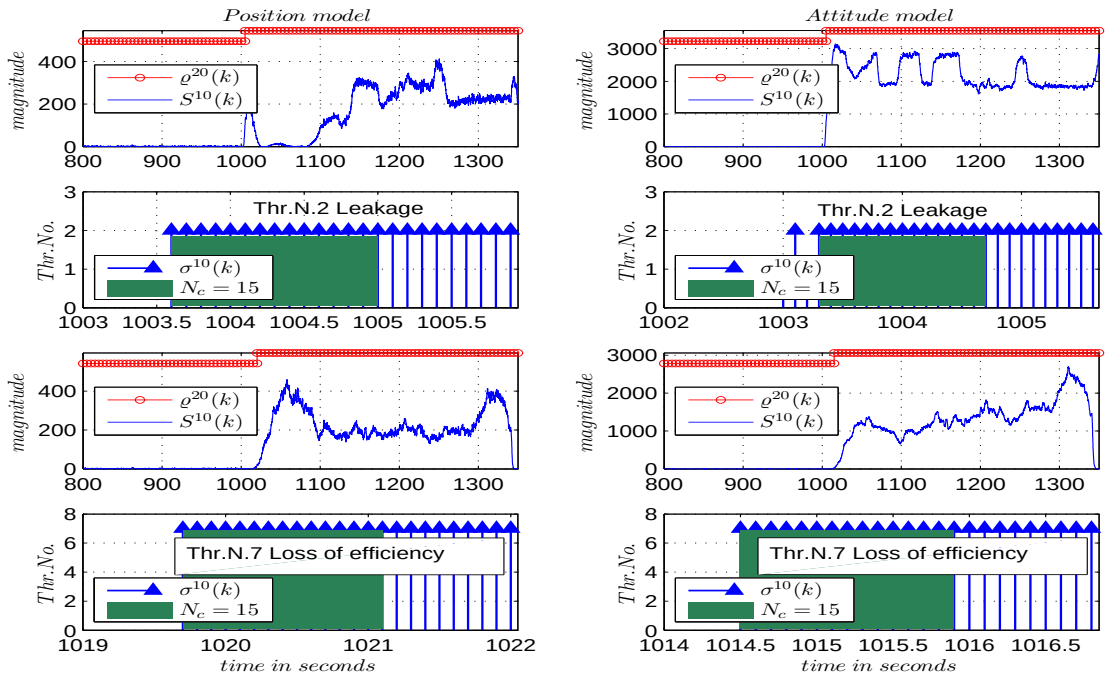


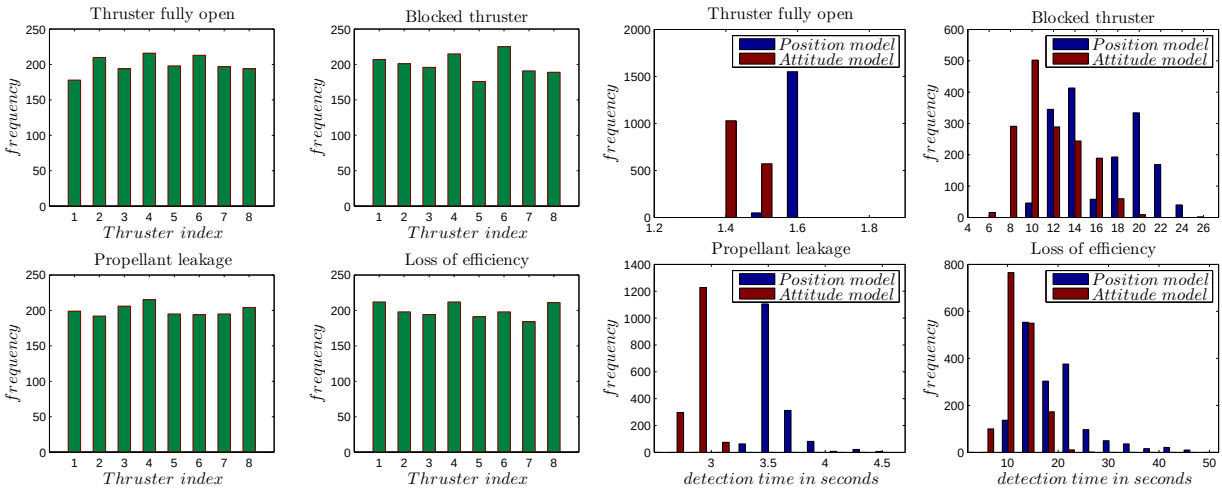
Figure 3.10 – Behaviour of the internal signals of the position (on the left) and attitude (on the right) model-based FDI scheme, respectively

Table 3.1 – Evaluated FDI performance indices based on 4x1600 Monte Carlo runs

Criterion/ Scenario	**Position model-based FDI**				**Attitude model-based FDI**			
	Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 1**	**Case 2**	**Case 3**	**Case 4**
$mean(\tau_d)$	1.6	16.3	3.6	18.8	1.4	11.7	2.9	12.2
$std(\tau_d)$	0.017	3.803	0.167	6.594	0.048	2.895	0.076	3.064
$mean(\tau_i)$	3.4	17.9	5.5	20.4	3.6	15.0	5.5	15.6
$std(\tau_i)$	0.207	3.799	0.399	6.592	0.237	3.231	0.459	3.456
$p_f/p_{nd}/p_i$	0/0/1	0/0/1	0/0/1	0/0/1	0/0/1	0/0/1	0/0/1	0/0/1

In order to better appreciate the results presented in Table 3.1, histogram plots graphically demonstrate the distributions of the detection (τ_d), isolation (τ_i) and pure isolation (t_i-t_d) delays. Figure 3.11b shows a comparison of the obtained results in terms of detection times, Fig. 3.12a in terms of isolation times and finally Fig. 3.12b in terms of pure isolation times. This visual representation allows to evaluate the FDI performances in terms of minimum and maximum detection/isolation times, as well as to observe the median values.

It can be seen from Fig. 3.11b that (as expected) the FDI unit based on the attitude model presents a greater sensitivity towards all the faulty situations. This can be easily explained by the fact that the attitude dynamics reacts more quickly to small faults. By closer examining Fig. 3.12a, it can be revealed that the final performance (isolation times) of both FDI schemes are only slightly different from each other. Furthermore, from Fig. 3.12b, it can be seen that in terms of pure isolation times, the position model-based approach performs better. This can be simply explained by the fact that the position model-based residual evolves more likely in the direction of the fault.



(a) Histograms of the thruster indices distribution (b) Histograms for detection delays

Figure 3.11 – Histograms for thruster indices distribution and detection delays

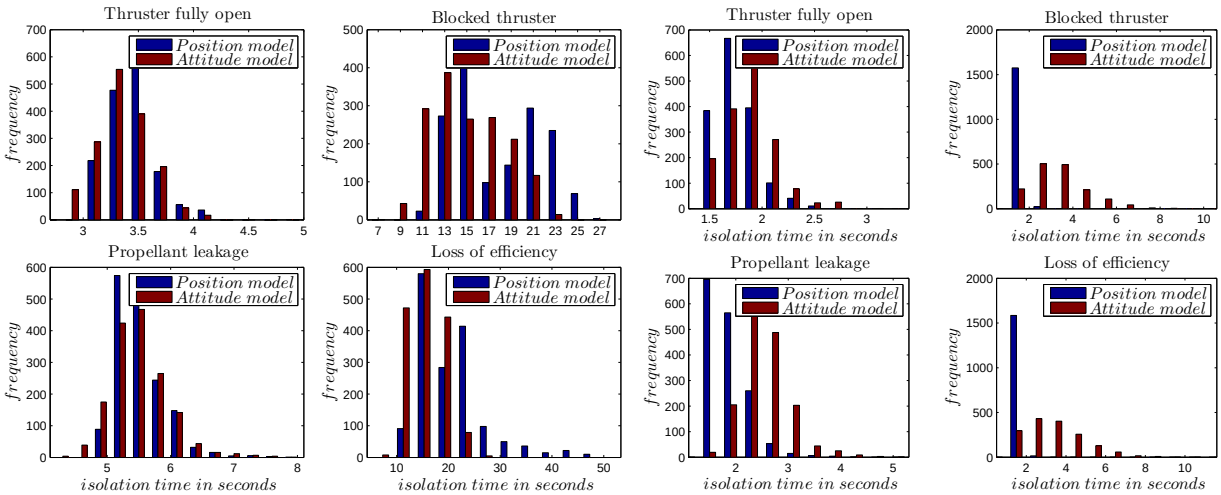
3.3.3 Concluding Remarks on the Obtained FDI Results

The obtained results indicate that both proposed model-based FDI schemes are effective and applicable for on-board implementation. They also show that all considered fault scenarios are covered with the suggested model-based FDI schemes, i.e., they are able to unambiguously isolate all considered faults with high probability. However, this is in contrast with the classical FDIR approaches used in satellite systems. Moreover, the carefully selected performance indicators also reveal that the position model-based scheme tends to achieve very similar FDI performance as the scheme based on the attitude model.

The position model-based FDI scheme succeeded thanks to the judiciously chosen linear model, i.e., a model that takes into account both the rotational and translational motions of the chaser. In other words, the dynamics of the attitude of the chaser is not modeled, but the chaser quaternion is introduced in the residual computation (quaternion-based force vector scheduling, see equation (3.1) for details). This allows to propose a fault diagnosis solution with a very similar performances to those based on the attitude model. Moreover, the position model is naturally robust against the model uncertainties, such as center of mass and inertia, whilst the attitude model not. The linearity of the attitude model during the fault presence is also questionable. Since only one observer is used for both fault detection and isolation, the computational burden is kept relatively low which is an a prior condition for on-board implementation.

It should be also note that the occurrence of incipient or relatively small size thruster faults (e.g., small propellant leakage or thrust loss) may be covered by (robust) control actions, which lead to the selection of the minimum interval limits for $\hat{m}_{leak}$ and $\hat{m}_{loss}$, respectively. The early detection of such faults is clearly more challenging. Another problem can arise when a blocked-closed thruster is not commanded and thus a fault detection is almost impossible. Such behaviour was not observed, since the TMF unit respects the thruster non-linearities (minimum On/Off times) of each thruster in the set.

Finally, all considered faults are detected and isolated by the proposed FDI units within a reasonable time (see the results presented in Table 3.1), i.e., within a time interval which allows the GNC system to keep its required performance (e.g., in terms of pointing accuracy and



(a) Histograms for isolation delays (b) Histograms for pure isolation delays

Figure 3.12 – Histograms for isolation and pure isolation delays

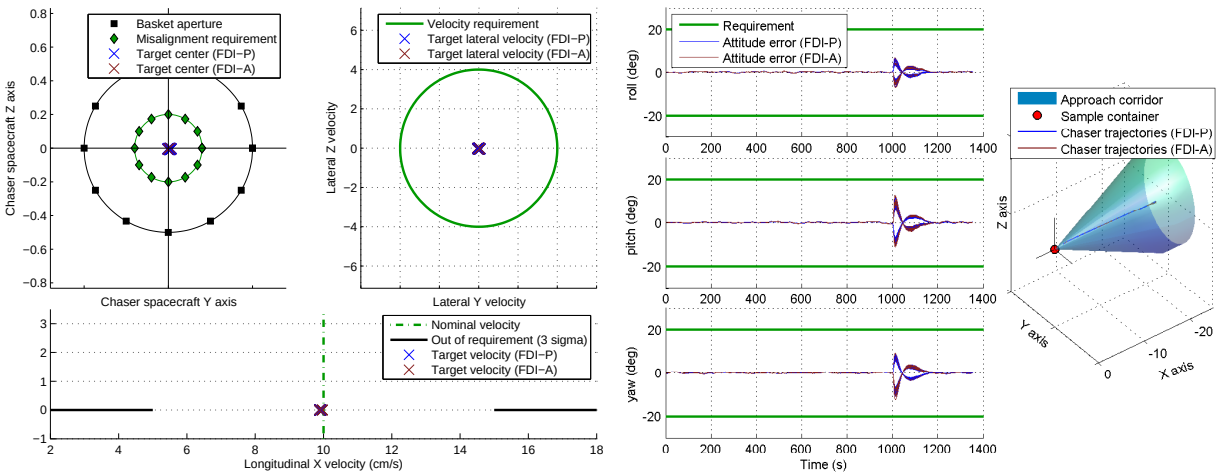
trajectory keeping) and meet the final capture requirements (see Chapter 2). The purpose of the next section is to illustrate the impact of the isolation delay on the recovery action.

3.4 Recovery Aspects

After the faulty thruster has been successfully detected and isolated by the FDI unit, the system can attempt to recover from the fault. The strategy of recovery is the last element of the proposed fault tolerant scheme and is ensured by switching to the fault-free thruster, thanks to the full hardware redundancy in thrusters. More precisely, the strategy is based on redirecting the control input $\tilde{u}_i$ of the faulty thruster (with index 'i') from thruster set 'A' to the thruster in the redundant set 'B'. This makes the fault recovery without any change in the nominal controller or/and in the in-placed TMF.

Without a valve to switch off the faulty thruster, there is only one way to control the spacecraft, i.e., try to on-line compensate the force and torque of the faulty thruster. However, this would lead to a drastic increase of the propellant consumption which is already very constrained by the travel to Mars. Therefore, a thruster which has been failed must be switched off by a dedicated Thruster Latch Valve (TLV). Fortunately, each thruster is equipped with a TLV leading the proposed FDIR solution to be a viable solution. Note that, in contrast to the "half-satellite" strategy, this approach can be (re-)used for each thruster separately, and thus, significantly increase the fault coverage capabilities.

In the following, a set of 4×100 randomly chosen simulation scenarios from the Monte Carlo campaign presented in Section 3.3.2 is considered. This set is used to analyse the effect of the isolation delay on the fault recovery, and thus, on the overall GNC performance as well as on the final capture requirements. For each scenario, two simulations are required. One for the recovery built on the position model-based FDI unit (further denoted as FDI-P) and the other built on the attitude model-based FDI scheme (further denoted as FDI-A). In total, a set of 800 simulations has been considered.



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser's attitude error (left) and trajectory inside the rendezvous corridor (right)

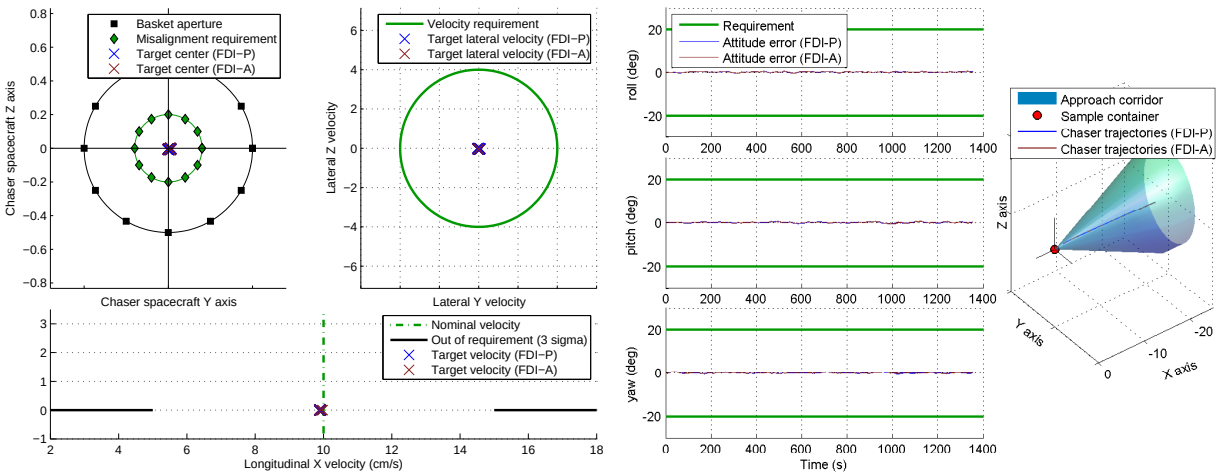
Figure 3.13 – Capture position requirements and GNC performances for fault Case 1

Figures 3.13-3.18 illustrate the fault recovery aspects of the two FDIR strategies, i.e., the one based on the FDI-P and the other based on FDI-A scheme, respectively. The capture conditions in terms of position and velocities are given in Fig. 3.13a, Fig. 3.14a, Fig. 3.16a, and Fig. 3.17a for fully open thruster, blocked-closed thruster, leaking thruster and loss of efficiency thruster fault, respectively. Figure 3.13b, Fig. 3.14b, Fig. 3.16b and Fig. 3.17b illustrate, that in all faulty cases, the chaser maintains the required trajectory, i.e., stays inside the rendezvous corridor (right on the figures), and that the chaser keeps its attitude pointing towards the target leading to a successful capture (left on the figures). Finally, Fig. 3.15 and Fig. 3.18 show that the proposed strategy is able to meet the required 3σ capture accuracy in terms of angular misalignment and angular rate errors.

The obtained simulation results on the recovery aspects indicate that the isolation performances given by Table 3.1, for both FDI schemes (FDI-P and FDI-A), are reasonable when considering the coupling of the isolation delay with the GNC system performance and capture accuracy. In other words, the obtained results suggest that both FDI units are able to perform fault detection/isolation (for the considered fault profiles) within a time interval less than the time during which the system becomes saturated (e.g., the LIDAR sensor is out of sight) or the control accuracy becomes intolerable (e.g., the capture requirements are not met).

3.5 Conclusion

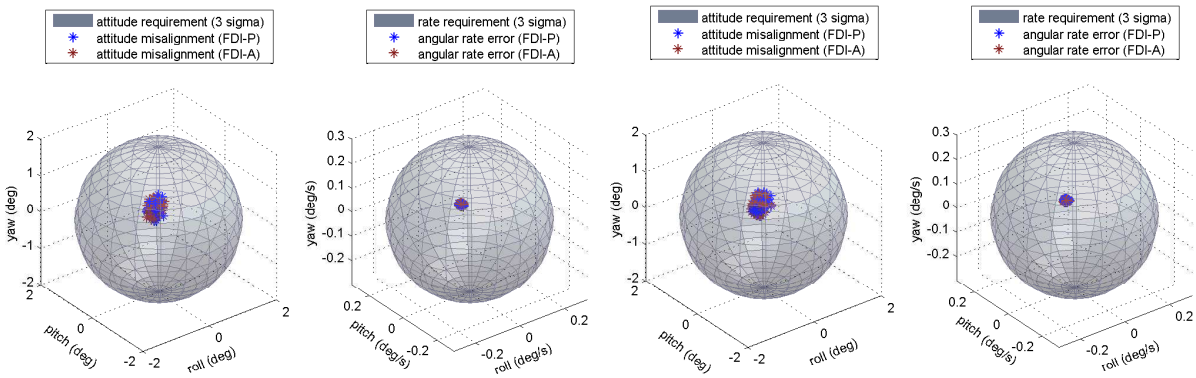
This chapter presented a complete design and implementation of two different model-based FDIR strategies for thruster fault diagnosis and accommodation (recovery). The focus of both approaches is on the robustness issue against the unknown time-varying delays induced by the propulsion drive electronics and uncertainties on thruster rise times. The idea is to transform these unstructured uncertainties into unknown inputs and to decouple them from the residual by means of EA technique. Two polytopic transformations to the original system are introduced. The first transformation is based on the Cayley-Hamilton theorem whereas the second relies on the h-order Taylor series expansion. Based on these transformations, the effect of the uncertain-



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser's attitude error (left) and trajectory inside the rendezvous corridor (right)

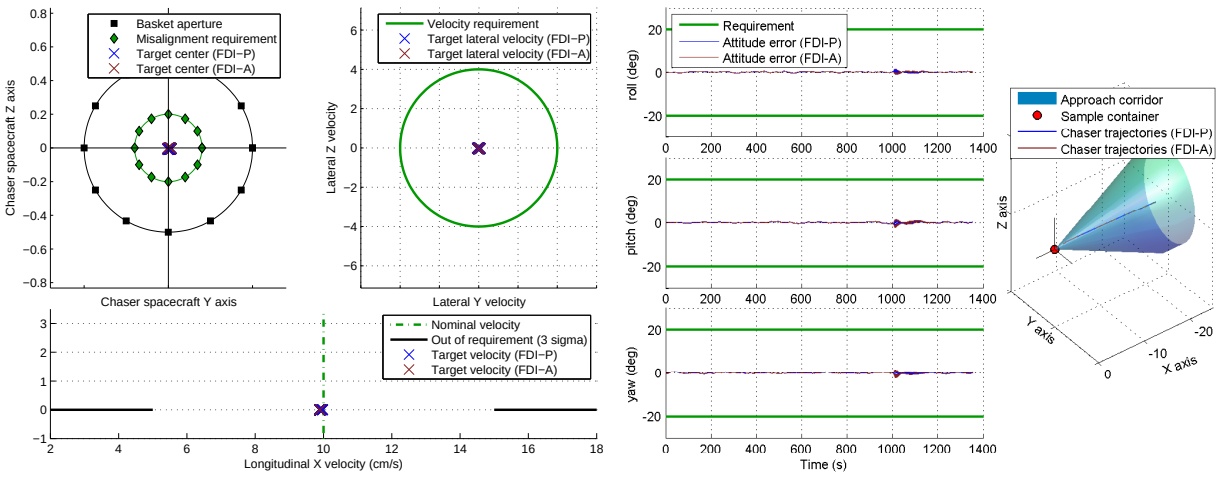
Figure 3.14 – Capture position requirements and GNC performances for fault Case 2



(a) Angular misalignment (left) and angular rate error (right) at capture

(b) Angular misalignment (left) and angular rate error (right) at capture

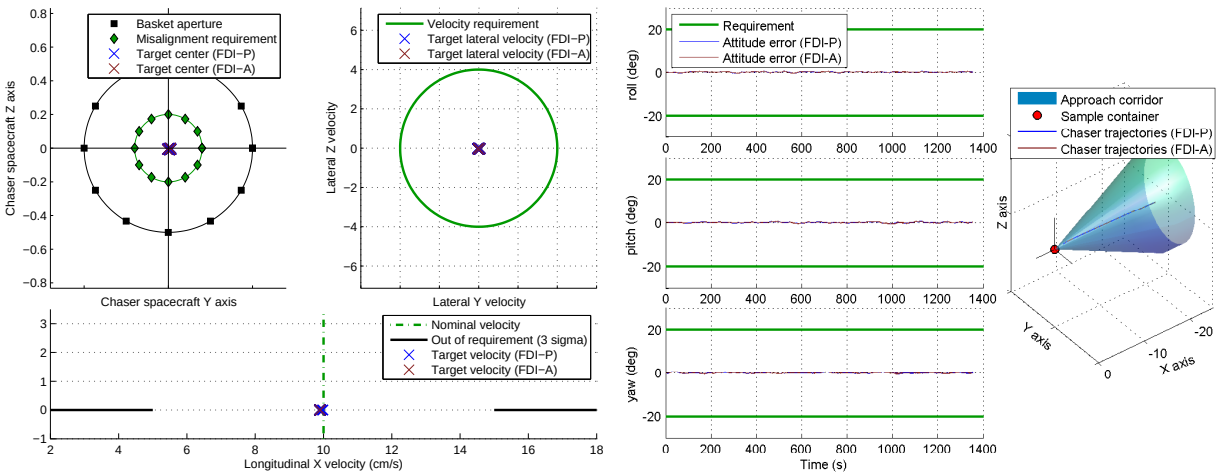
Figure 3.15 – Capture angular requirements for fault Case 1 and Case 2



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser's attitude error (left) and trajectory inside the rendezvous corridor (right)

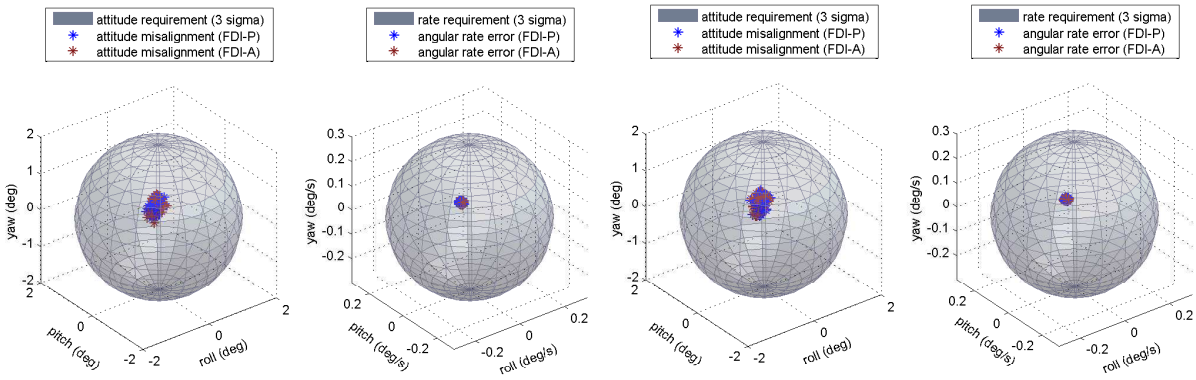
Figure 3.16 – Capture position requirements and GNC performances for fault Case 3



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser's attitude error (left) and trajectory inside the rendezvous corridor (right)

Figure 3.17 – Capture position requirements and GNC performances for fault Case 4



(a) Angular misalignment (left) and angular rate error (right) at capture

(b) Angular misalignment (left) and angular rate error (right) at capture

Figure 3.18 – Capture angular requirements for fault Case 3 and Case 4

ties on the state is summarized as an unknown input linked with its corresponding distribution matrix. The estimation of the complex unknown input distribution matrix can be considered as a contribution to the theory. The robust (in the sense of unknown input decoupling) observer-based residual generation for FDI is achieved by assigning some left eigenvectors of the observer to be orthogonal to the unknown input directions (columns of the distribution matrix).

The faulty thruster isolation is achieved by cross-correlation-like test between the residual signal and the commanded thruster open rates. To reduce computational burden, the isolation test is based on a sliding window and thus having a low computational complexity which is a prior condition for an on-board implementation. Fault accommodation is achieved by employing the additional hardware redundancy in the thrusters, i.e., as soon as the faulty thruster is isolated by the FDI unit, it is switched off using a dedicated thruster latch valve and the redundant thruster from the back-up set is used instead. This makes the fault recovery without any change in the nominal controller or/and TMF. Additionally, the thruster fault isolation is made without requiring any valve position sensors. The core element of this chapter is the judiciously chosen

position model. This model was used to design the first FDI scheme and was compared (in terms of well established FDI performance indices) to the second one, the attitude model-based scheme.

A Monte Carlo simulation campaign has been performed under realistic conditions considering measurement noises, delays, spatial disturbances and parameter uncertainties. Four different fault scenarios were injected throughout simulations. The obtained results demonstrated hight reliability (no false alarms) and the efficiency (reasonable detection times) of the proposed FDI schemes. Moreover, the simulation campaign on recovery issues revealed that the isolation delay of both FDI schemes has only minor effect on the GNC system performance and that the final capture requirements can be fully met since the system is recovered to its pre-fault condition (nominal operation). The following chapter addresses an enhanced fault detection, isolation and accommodation solution based on an active FTC scheme.

Chapter 4

Active FTC Approach for a New Thruster Configuration without Redundant Set

"All stable processes we shall predict. All unstable processes we shall control."
— John von Neumann, Hungarian-born mathematician

This chapter addresses the design and implementation of an active fault tolerant control system strategy to detect, unambiguously isolate and accommodate a single thruster fault occurring in the thruster-based propulsion system. Since the thruster configuration used in the previous chapter has not enough degrees of freedom to deal with such an advanced solution, a new layout of thrusters is considered. Key features of the proposed method are the use of the following components: a fault detector based on eigenstructure assignment technique for robust and quick fault detection, a bank of nonlinear unknown input observers with dynamics assignment together with an extended Kalman filter-based torque bias estimator for fault isolation and an online control allocation unit scheduled by the fault isolation scheme for fault tolerance. A Monte Carlo campaign is conducted in the context of the terminal rendezvous phase. Mission oriented criteria demonstrate that the proposed FTC strategy is able to cope with a large class of thruster faults, despite the presence of various types of uncertainties.

4.1 New Thruster Configuration

The considered thruster configuration in this chapter is different from the baseline MSR configuration introduced in Chapter 3. It is a special one designed by Thales Alenia Space industries, in order to study active fault-tolerant strategies. This configuration is composed of $N = 12$ thrusters and is physically organised in four groups, see Fig. 4.1 for illustration.

This configuration disposes of some degrees of freedom to achieve fault tolerance (functional redundancy). Particularly, the set of 12 thrusters is placed on the chaser such that the nominally attainable set Ω_a of propulsion torques $\boldsymbol{T}$ and forces $\boldsymbol{F}$ is likewise attainable by combining the thrusts of any $N - 1 = 11$ thrusters. From practical viewpoint, it means that it is possible

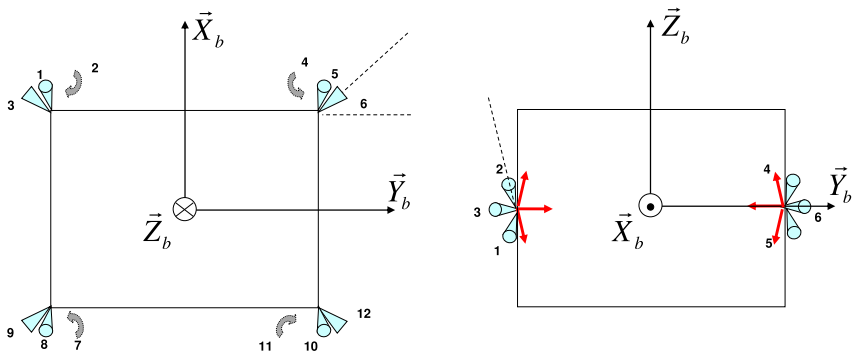


Figure 4.1 – Thruster configuration of the chaser spacecraft

to achieve the required capture accuracy and the necessary GNC performance with only 11 (healthy) thrusters. This fact will be justified in the next section. The main drawback of this new thruster configuration is, that in terms of FTC, it requires a fault isolation function and also that the TMF and/or the already in-placed controller must be changed in order to cope with the fault.

Considering the thruster configuration illustrated in Fig. 4.1 by analysing the sensitivity matrices $\boldsymbol{B}_F$ and $\boldsymbol{B}_T$ (attached to this configuration) in terms of directional properties, the following can be concluded: the torque directions of the thrusters having index inside the sets $\mathcal{S}_{Tk}, k = 1, \ldots, 4$ are the same and those having index inside the set $\mathcal{S}_{T5}$ are similar. In our case, the above subsets are defined as follows

$$\begin{aligned} &\mathcal{S}_{T1} = \{1, 11\}, \quad \mathcal{S}_{T3} = \{4, 8\}, \quad \mathcal{S}_{T5} = \{3, 6, 9, 12\} \\ &\mathcal{S}_{T2} = \{2, 10\}, \quad \mathcal{S}_{T4} = \{5, 7\}, \end{aligned} \tag{4.1}$$

In terms of force directions, the following property is revealed

$$\begin{aligned} &\boldsymbol{b}_{F1} = -\boldsymbol{b}_{F11}, \quad \boldsymbol{b}_{F4} = -\boldsymbol{b}_{F8}, \quad \boldsymbol{b}_{F3} = -\boldsymbol{b}_{F12} \\ &\boldsymbol{b}_{F2} = -\boldsymbol{b}_{F10}, \quad \boldsymbol{b}_{F5} = -\boldsymbol{b}_{F7}, \quad \boldsymbol{b}_{F6} = -\boldsymbol{b}_{F9} \end{aligned} \tag{4.2}$$

which means that thruster pairs given by $\mathcal{S}_{Tk}, k = 1, ..., 4$ produce exactly opposite forces. The last thruster group, i.e., $\mathcal{S}_{T5}$, has the following properties

$$\boldsymbol{b}_{F3} \cdot \boldsymbol{b}_{F6} = 0, \quad \boldsymbol{b}_{T3} \approx -\boldsymbol{b}_{T6} \approx -\boldsymbol{b}_{T9} \approx \boldsymbol{b}_{T12} \tag{4.3}$$

where " $\cdot$ " denotes the dot product. Relations in (4.3) mean that thrusters belonging to the $\mathcal{S}_{T5}$ group produce a) forces perpendicular to the forces of their neighbours b) nearly collinear torques. Directional properties given by (4.1)-(4.3) are visualised in Fig. 4.2 and will be later used to derive an explicit fault isolation strategy.

Note, that not only the number of thrusters and the absence of the redundant set differs from the configuration considered in Chapter 3, but also the fact that there are two thruster pairs in the fifth group, which produce torques in a very similar directions. This makes the fault diagnosis task (especially the isolation) very challenging.

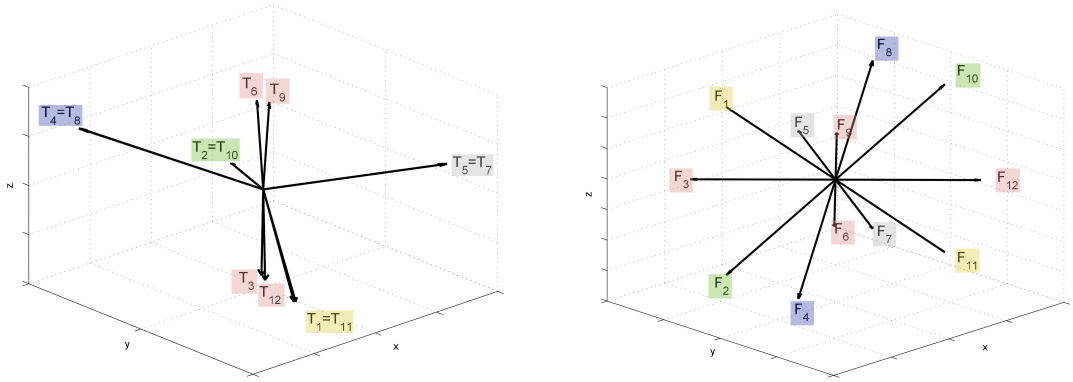


Figure 4.2 – Torque directions (left) and force directions (right)

4.1.1 Feasibility of the Attainable Forces and Moments

Let Ω_a be the set of attainable forces/moments linked with the here investigated thruster configuration and Ω_a^k be the set of attainable forces/moments using all thrusters but the k^{kt} one, then $\Omega_a^k \subseteq \Omega_a, \forall k \in \mathcal{S}_{all}$. Then, it is revealed that sets $\Omega_a^k, \forall k \in \mathcal{S}_{all}$ are very close to Ω_a. This can be also illustrated by a simple example, see Fig. 4.7.

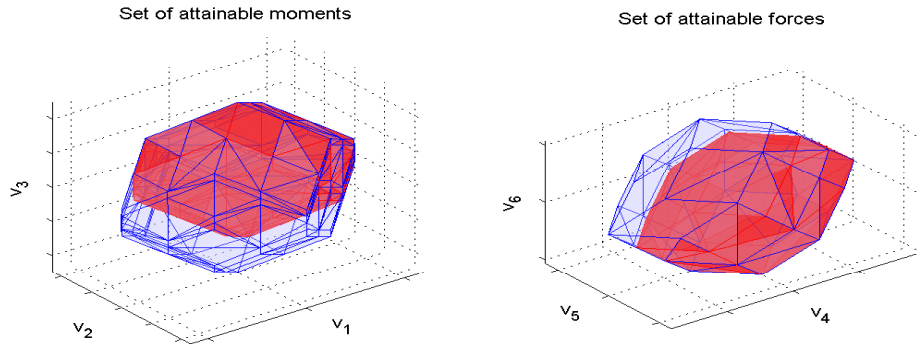


Figure 4.3 – Set of attainable moments (left) and forces (right) using all 12 thrusters (blue polyhedron) and using only 11 thrusters (red polyhedron) and in both cases taking into account the thruster limits

This figure illustrates the set of attainable moments and forces in the case of a single example using all the 12 thrusters (i.e., the set Ω_a) and in the case when thruster No.1 is not considered (i.e., the set Ω_a^1). Note, that these sets were generated taking into account the upper thruster limits, see the discussion at the beginning of Chapter 3.

Figure 4.7 shows that only a small portion of the "quasi control authority" is lost when considering Ω_a^1 for control[1]. Thus, it is guaranteed that this new thruster configuration is capable of achieving admissible GNC and capture/rendezvous performances, whenever 11 thrusters are available, that is for all $\Omega_a^k, \forall k \in \mathcal{S}_{all}$.

Remark 4.1. *The MIB constraint was not taken into account when computing Fig. 4.7. Basically, it would create a dead zone-like subset (polyhedron) around the origin of the coordinate system. This, however, does not invalidate the claims mentioned above.*

[1]It should be noted, that Fig. 4.7 illustrates only the thruster configuration physical capabilities and not the real control authority which is obviously dependent on the selected control law (controller and/or TMF).

4.2 Context and motivations

Following the previous discussion, it seems clear that the major problem turns out to be the design of FTC scheme able to detect, isolate and accommodate a faulty thruster. This is the main purpose of this chapter where an active FTC solution is provided. The idea is that instead of trying to redesign the already in-placed nominal controller (in the presence of thruster faults), the control allocation module is reconfigured with the use of the baseline 6DOF control law, such that the control effort is redistributed (re-allocated) to the remaining operational thrusters.

Note, that the problem of designing an active FTC system for thruster faults has been rarely studied for space systems (or very few papers have been published). In terms of model-based FDI, numerous techniques have been studied in the past decades in the academic community, see Chapter 1 or [19, 60, 231] for good surveys.

Additionally to works presented in Chapter 1, one can mention [246] that proposes a torque bias vector matching FDI algorithm. The torque bias is estimated using an EKF and directly matched with the torque directions of each thruster. The main drawback of this approach is that it is unable to consider a thruster configuration where some thrusters generate same or very similar torques, which is the case of the new thruster configuration presented earlier. A similar idea is presented in [5], where instead of estimating the torque bias, the sliding mode injection term is matched with the thruster directions. This method has similar drawbacks like the previous method. Additionally, the isolation performance strongly depends on the measurement noise. In [240], a robust model–based H_∞/H_- FDI filter is used for thruster fault detection and fault isolation is performed using a bank of linear thruster–direction decoupling observers.

In the aero-space community, the control allocation technique is probably the most "ready to be implemented" FTC approach. The major reason is that, even if the technique has been used only for FTC purpose for a few space experiments, the computational complexity is already within the limits of today's off-the-shelf embedded computer systems, see [20, 21, 99, 127, 156, 157, 216, 219]. Thruster faults can be dealt with using CA principle so that it is not required to re-design the control law itself. A consequence is that CA can be used as a FTC solution with a little extra effort on the original techniques. This chapter follows this idea.

4.3 Robust Fault Detector Design

Since in any FTC scheme, it is required a fault detection and isolation scheme, this section addresses the design of a robust fault detector. The fault detector shall indicate the fault occurrence in the thruster-based propulsion system. The proposed fault detector is based on a robust residual generator and a statistical decision test that evaluates the residual. The residual is designed such that it lends robustness against the uncertain delay $\tau(t)$ introduced in Section 2.2.3. Following the reasoning about the position model-based fault detector in Chapter 3, the proposed residual generator in this chapter is based on the relative position model[2]. Robustness is achieved by employing a different approach, i.e., the uncertain delay

[2]This, however, poses no limits on the applicability of the proposed fault detector approach to position model only. In fact, attitude model can be equally used. The usage of the position model will be further justified in Section 4.4.

is modelled using a first-order Padé approximation. This uncertainty is next approximated in terms of unknown inputs and decoupled by means of an EA technique. The whole design procedure is derived in the continuous time domain rather than in the discrete time as it was the case in Chapter 3.

4.3.1 Problem Setting

Consider the position model given by (3.3) with additive thruster fault model (3.1) and input delays (3.8) (the index "p" is omitted here for clarity)

$$\begin{cases} \dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) + \boldsymbol{E}_f\boldsymbol{f}(t) \\ \boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{4.4}$$

The system input $\boldsymbol{u}$ is considered in the continuous fashion as

$$\boldsymbol{u}(t) = \boldsymbol{u}_c(t - \tau(t)) \tag{4.5}$$

where $\boldsymbol{u}_c(t) = \boldsymbol{u}_c(k), \forall t \in [kT, (k+1)T)$ is the continuous time version (piecewise-continuous) of the discrete time system input $\boldsymbol{u}_c(k)$, see (3.9) if necessary.

Compared to (3.8), it can be noted that, here the discrete time unknown delay τ_k is considered to be a time-varying piecewise continuous (continuous from the right) delay $\tau(t) = \tau(k)$, $\forall t \in [kT, (k+1)T)$. Thus, (4.5) is an equivalent representation of (3.8) in the continuous time domain.

The robust residual generation problem is then formulated as follows:

Problem 4.1. *Design a continuous time residual generator of the form*

$$\boldsymbol{r}(s) = \boldsymbol{H}_y(s)\boldsymbol{y}(s) + \boldsymbol{H}_u(s)\boldsymbol{u}_c(s) \tag{4.6}$$

with $\boldsymbol{H}_y/\boldsymbol{H}_u$ being observer-based transfer functions, such that the residual signal $\boldsymbol{r}$ lends robustness against the uncertain time-varying delay $\tau(t)$.

4.3.2 Derivation of the Solution

In order to solve Problem 4.1, the influence of the uncertain time-varying delay is first expressed as an unknown input. This is achieved by using a first-order Padé approximation and introducing a new augmented state space description. Second, the unknown input is decoupled by means of EA technique.

To proceed, consider the transfer function

$$\mathcal{H}(s) = \frac{\boldsymbol{u}(s)}{\boldsymbol{u}_c(s)} = e^{-\tau(t)s} \tag{4.7}$$

of the time delay $\tau(t)$ being an irrational transfer. Therefore, it is useful to substitute $e^{-\tau(t)s}$ with an approximation in form of a rational transfer function. The most common approximation

is the Padé approximation

$$e^{-\tau(t)s} \doteq \frac{1 - k_1 s + k_2 s^2 + \ldots \pm k_p s^p}{1 + k_1 s + k_2 s^2 + \ldots + k_p s^p} \tag{4.8}$$

where p is the order of the approximation and the coefficients k_i are functions of p.

Here, a first-order Padé approximation of the time delay is considered when the Padé coefficients become: $k_1 = \frac{\tau(t)}{2}$ and $k_i = 0$, $i = 2, \ldots, p$. The irrational transfer can be then approximated as

$$e^{-\tau(t)s} \doteq \frac{1 - \frac{\tau(t)}{2}s}{1 + \frac{\tau(t)}{2}s} \tag{4.9}$$

If this approximation is considered for all system inputs, then the transfer function (4.9) is equivalent to the following state space representation

$$\begin{cases} \dot{\boldsymbol{x}}_d(t) = \boldsymbol{A}_d(\tau)\boldsymbol{x}_d(t) + \boldsymbol{B}_d\boldsymbol{u}_c(t) \\ \boldsymbol{u}(t) = \boldsymbol{C}_d(\tau)\boldsymbol{x}_d(t) + \boldsymbol{D}_d\boldsymbol{u}_c(t) \end{cases} \tag{4.10}$$

where $\boldsymbol{x}_d(t)$ is the delayed state and the matrices $\boldsymbol{A}_d(\tau), \boldsymbol{B}_d, \boldsymbol{C}_d(\tau)$ and $\boldsymbol{D}_d$ are given as follows

$$\boldsymbol{A}_d(\tau) = -\tfrac{2}{\tau(t)}\boldsymbol{I}, \quad \boldsymbol{B}_d = \boldsymbol{I}, \quad \boldsymbol{C}_d(\tau) = \tfrac{4}{\tau(t)}\boldsymbol{I}, \quad \boldsymbol{D}_d = -\boldsymbol{I}$$

The augmented state-space description of the system (4.4) and the delayed inputs (4.10) with the state vector $\boldsymbol{z}^T = \left[\boldsymbol{x}^T \boldsymbol{x}_d^T\right]$ is:

$$\begin{cases} \dot{\boldsymbol{z}}(t) = \hat{\boldsymbol{A}}(\tau)\boldsymbol{z}(t) + \hat{\boldsymbol{B}}\boldsymbol{u}_c(t) + \hat{\boldsymbol{E}}_f\boldsymbol{f}(t) \\ \boldsymbol{y}(t) = \hat{\boldsymbol{C}}\boldsymbol{z}(t) \end{cases} \tag{4.11}$$

where

$$\hat{\boldsymbol{A}}(\tau) = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B}\boldsymbol{C}_d(\tau) \\ \boldsymbol{0} & \boldsymbol{A}_d(\tau) \end{bmatrix}, \quad \hat{\boldsymbol{B}} = \begin{bmatrix} \boldsymbol{B}\boldsymbol{D}_d \\ \boldsymbol{B}_d \end{bmatrix}, \quad \hat{\boldsymbol{C}} = \begin{bmatrix} \boldsymbol{C} & \boldsymbol{0} \end{bmatrix}, \quad \hat{\boldsymbol{E}}_f = \begin{bmatrix} \boldsymbol{E}_f \\ \boldsymbol{0} \end{bmatrix}$$

It can be seen, that thanks to the chosen state-space representation (4.10), the uncertainty τ is present only in $\hat{\boldsymbol{A}}(\tau)$. The task now is to decompose this matrix into a constant and parameter-varying part.

More precisely, the task is to decompose the matrix $\hat{\boldsymbol{A}}(\tau)$ in the following form

$$\hat{\boldsymbol{A}}(\tau) = \hat{\boldsymbol{A}}_0 + \Delta\hat{\boldsymbol{A}}(\tau) \tag{4.12}$$

where $\hat{\boldsymbol{A}}_0$ is a constant matrix and $\Delta\hat{\boldsymbol{A}}(\tau)$ is the parameter-varying (uncertain) part of $\hat{\boldsymbol{A}}(\tau)$.

Let be considered that $\tau(t)$ can be expressed as

$$\tau(t) = \tau_0 + \delta(t) \ : \ |\delta(t)| \leq \bar{\delta} \tag{4.13}$$

where $\tau_0 > 0$ is the nominal delay, $\delta(t)$ is the variation around τ_0, and $0 < \bar{\delta} < \tau_0$ is the upper bound of the variation part.

Proposition 4.1. *The inverse of the uncertain time-delay $\tau(t)$ can be expressed as*

$$(\tau(t))^{-1} = \big(\tau_0 + \delta(t)\big)^{-1} = \frac{1}{\tau_0} - \frac{1}{\tau_0}\delta^*(t) \tag{4.14}$$

where $\delta^*(t) = \frac{\delta(t)}{\tau_0+\delta(t)}$.

Proof. Let $a \in \mathbb{R}$ and $b \in \mathbb{R}$ be two real scalars, where $a \neq 0$ and $a + b \neq 0$. Then based on Miller's lemma [196] (see Appendix A) the following holds

$$(a+b)^{-1} = a^{-1} - a^{-1}\frac{b}{a+b} \tag{4.15}$$

Using (4.13) and (4.15), Proposition 4.1 yields. ■

Based on Proposition 4.1, (4.12) is defined as follows

$$\hat{\boldsymbol{A}}_0 = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B}\boldsymbol{C}_d^{\tau_0} \\ \boldsymbol{0} & \boldsymbol{A}_d^{\tau_0} \end{bmatrix}, \qquad \Delta\hat{\boldsymbol{A}}(\tau) = \begin{bmatrix} \boldsymbol{0} & -\boldsymbol{B}\boldsymbol{C}_d^{\tau_0} \\ \boldsymbol{0} & -\boldsymbol{A}_d^{\tau_0} \end{bmatrix}\delta^*(t) \tag{4.16}$$

where $\boldsymbol{A}_d^{\tau_0} = -\frac{2}{\tau_0}\boldsymbol{I}$ and $\boldsymbol{C}_d^{\tau_0} = \frac{4}{\tau_0}\boldsymbol{I}$.

Now, the parameter-varying part $\Delta\hat{\boldsymbol{A}}(\tau)$ can be expressed as an unknown input $\boldsymbol{d}(t)$, entering the augmented dynamics (4.11) through $\hat{\boldsymbol{E}}_d$, by:

$$\Delta\hat{\boldsymbol{A}}(\tau)\boldsymbol{z}(t) = \begin{bmatrix} \boldsymbol{0} & -\boldsymbol{B}\boldsymbol{C}_d^{\tau_0} \\ \boldsymbol{0} & -\boldsymbol{A}_d^{\tau_0} \end{bmatrix}\delta^*(t)\boldsymbol{z}(t) = \hat{\boldsymbol{E}}_d\boldsymbol{d}(t) \tag{4.17}$$

where

$$\hat{\boldsymbol{E}}_d = \begin{bmatrix} -\boldsymbol{B}\boldsymbol{C}_d^{\tau_0} \\ -\boldsymbol{A}_d^{\tau_0} \end{bmatrix}, \qquad \boldsymbol{d}(t) = \delta^*(t)\boldsymbol{x}_d(t) \tag{4.18}$$

Finally, the uncertain system described by (4.11) can be rewritten as an LTI system with unknown inputs

$$\begin{cases} \dot{\boldsymbol{z}}(t) = \hat{\boldsymbol{A}}_0\boldsymbol{z}(t) + \hat{\boldsymbol{B}}\boldsymbol{u}_c(t) + \hat{\boldsymbol{E}}_f\boldsymbol{f}(t) + \hat{\boldsymbol{E}}_d\boldsymbol{d}(t) \\ \boldsymbol{y}(t) = \hat{\boldsymbol{C}}\boldsymbol{z}(t) \end{cases} \tag{4.19}$$

This model is an equivalent representation of the initial model (4.4)-(4.5) which approximates the effect of the uncertain time-varying delay $\tau(t)$ on the state in terms of an unknown input $\boldsymbol{d}(t)$ and a first-order Padé approximation. The problem then turns out to be the design of the fault detector.

To proceed, consider the following residual generator based on a full-order observer

$$\begin{cases} \dot{\hat{\boldsymbol{z}}}(t) = (\hat{\boldsymbol{A}}_0 - \hat{\boldsymbol{L}}\hat{\boldsymbol{C}})\hat{\boldsymbol{z}}(t) + \hat{\boldsymbol{B}}\boldsymbol{u}_c(t) + \hat{\boldsymbol{L}}\boldsymbol{y}(t) \\ \boldsymbol{r}(t) = \hat{\boldsymbol{Q}}\big(\boldsymbol{y}(t) - \hat{\boldsymbol{C}}\hat{\boldsymbol{z}}(t)\big) \end{cases} \tag{4.20}$$

where $\boldsymbol{r} \in \mathbb{R}^{n_r}$ is the residual signal and $\hat{\boldsymbol{z}}$ is the augmented state $\boldsymbol{z}$ estimate. The matrix $\hat{\boldsymbol{Q}} \in \mathbb{R}^{n_r \times n_y}$ is the output estimation error (residual) weighting matrix.

In order to solve Problem 4.1, the residual generator (4.20) must be designed such that

$$\boldsymbol{G}_{rd}(s) = \hat{\boldsymbol{Q}}\hat{\boldsymbol{C}}(s\boldsymbol{I} - \hat{\boldsymbol{A}}_0 + \hat{\boldsymbol{L}}\hat{\boldsymbol{C}})^{-1}\hat{\boldsymbol{E}}_d = \boldsymbol{0} \tag{4.21}$$

holds. To achieve this, the left EA approach introduced in Section 3.2.5 is used to compute $\hat{\boldsymbol{L}}$ and $\hat{\boldsymbol{Q}}$. The only difference using this (EA) approach for the continuous case is that the assigned eigenvalue set $\Lambda(\hat{\boldsymbol{A}}_0 - \hat{\boldsymbol{L}}\hat{\boldsymbol{C}}) = \{\lambda_i, i = 1, \ldots, n_z\}$ must belong to the stable left complex half plain, i.e., $\lambda_i \leq 0, \forall i$.

By this, the resulting residual $\boldsymbol{r}$ can be designed such that it is (approximately) decoupled from the unwanted effects of the time-varying delay $\tau(t)$. Furthermore, if the unknown input $\boldsymbol{d}$ is completely decoupled from $\boldsymbol{r}$, i.e., if (4.21) holds, then the resulting residual $\boldsymbol{r}$ is robust against the uncertain variations $\delta(t) \in (-\tau_0, \tau_0)$ of the delay $\tau(t)$, see (4.13).

Remark 4.2. *In the author's work [90], a robustness/sensitivity analysis campaign has been performed in order to compare the efficiency of two fault detectors, one based on the polytopic approach (Cayley-Hamilton) introduced in Section 3.2 and the other based on the Padé approach introduced in this section. The simulation results revealed that the Padé method offers greater sensitivity/robustness level towards all considered fault scenarios than the polytopic method.*

Implementation of the Residual Generator

A reasonable value of the nominal time delay τ_0 has been determined to be exactly one sampling interval, i.e., $T = 0.1$ s. Therefore, the distribution matrix $\hat{\boldsymbol{E}}_d$ is calculated with $\tau_0 = 0.1$ as in (4.18). This practically means that if the unknown input $\boldsymbol{d}$ is completely decoupled from $\boldsymbol{r}$, then the resulting residual $\boldsymbol{r}$ is robust against the uncertain time varying delay $\tau(t) \in (0, 0.2)$. Following the discussion in Section 3.2.5, the residual weighting matrix was determined to be $\hat{\boldsymbol{Q}} = \boldsymbol{I}$ and the dimension of the residual $n_r = 3$, i.e., $\boldsymbol{r} = [r_1, r_2, r_3]^T$. All the assigned eigenvalues were chosen to be close to -0.22. Finally, the residual generator (4.20) is converted to discrete time ($t = kT$) using a Tustin approximation [98] to be implemented within the nonlinear simulator of the MSR mission.

4.3.3 Residual Evaluation - Fault Detection

The residual evaluation function considered here is a slightly modified version of the scalar valued *GLR test for the variance*, see Appendix B. The proposed decision test $\varrho^{J_{th}}$ is defined by

$$\varrho^{J_{th}}(t) = \begin{cases} 1 & \text{if } S_w(\boldsymbol{r}(k)) > J_{th} \Rightarrow \text{fault declared} \\ 0 & \text{if } S_w(\boldsymbol{r}(k)) \leq J_{th} \Rightarrow \text{fault not present} \end{cases} \tag{4.22}$$

where

$$S_w(\boldsymbol{r}(k)) = \sum_{i=1}^{n_r} w_i S^{N_d}\left(r_i(k)\right) \tag{4.23}$$

is the weighted GLR algorithm with $w_i \geq 0$, $i = 1, \ldots, n_r$ being the normalized weight factors used to prioritize certain elements (axes) of the residual. $S^{N_d}\left(r_i(k)\right)$ is the estimated log likelihood of the GLR algorithm applied to the ith element of the residual signal $r_i(k)$ and evaluated on the sliding window N_d, i.e., using $k - N_d + 1, \ldots, k$ samples. The fixed threshold J_{th} is an

additional design parameter. The fault is declared at time t_d, i.e.,

$$t_d = \arg\inf_{t \geq t_0} \{\varrho^{J_{th}}(t) = 1\} \tag{4.24}$$

where $t_0 \geq 0$ is the time required for $\boldsymbol{r}$ to achieve steady state (settle down) when $\boldsymbol{\Psi}(t) = \mathbf{0}, \forall t \in [0, t_0)$.

The next step of the FDI algorithm is concerned by the isolation task which is addressed in the following section.

4.4 Design of the Isolation Scheme

Recall the thruster configuration properties given by (4.1)-(4.3) and taking into account the fact that thrusters cause both linear and rotational motions, a set of explicit rules can be derived to unambiguously isolate a single thruster fault. These rules are implemented on a hierarchical basis as follows:

i) The first stage is based on a bank of five NUIOs which is used to confine the faulty thruster into a single group $\mathcal{S}_{Tk}$ (subset of thrusters). The proposed NUIO approach is adopted because of its decoupling properties, adjustable error dynamics and ability to take into account both nonlinearities and uncertainties of the attitude dynamics.

ii) The second stage uses jointly an Extended Kalman Filter (in charge of estimating the torque bias due to the fault, torque bias matching or Wald's sequential test) and a residual/force vector matching approach (to uniquely isolate the faulty thruster within the already isolated subset $\mathcal{S}_{Tk}$).

4.4.1 Attitude Dynamics with Inertia Uncertainty

Let's recall here the model of the attitude dynamics (2.80) (no kinematic equations are considered in this chapter/approach) without taking into account the spatial disturbances (see Remark 3.1) and the time delay $\tau(t)$, i.e.,

$$\dot{\boldsymbol{\omega}}(t) = \boldsymbol{J}^{-1}\boldsymbol{B}_T\tilde{\boldsymbol{u}}_f(t) - \boldsymbol{J}^{-1}\boldsymbol{\omega}(t) \times \boldsymbol{J}\boldsymbol{\omega}(t) \tag{4.25}$$

where $\tilde{\boldsymbol{u}}_f(t) = (\boldsymbol{I} - \boldsymbol{\Psi}(t))\tilde{\boldsymbol{u}}(t)$ is the control input (thruster opening times) that takes into account the fault model given in (2.74).

Since the attitude model involves the inertia matrix $\boldsymbol{J}$ (and its inverse), robustness issue against uncertainties in $\boldsymbol{J}$ is a key problem. In aerospace industry, the real inertia is newer known precisely on-board, therefore the control laws are always validated in the presence of uncertainty on inertia to confront modelling errors. Similarly, in terms of FDI/FTC, it is important to analyse and incorporate into the design procedure the influence of the uncertain inertia for conditions of successful rendezvous.

To proceed, let $\boldsymbol{J}$ be of the general form

$$\boldsymbol{J} = \begin{bmatrix} J_{xx} & J_{xy} & J_{xz} \\ J_{xy} & J_{yy} & J_{yz} \\ J_{xz} & J_{yz} & J_{zz} \end{bmatrix} \tag{4.26}$$

First, a factorization of $\boldsymbol{J}$ is defined by introducing a diagonal matrix $\boldsymbol{J}_d \in \mathbb{R}^{9\times 9}$ with the uncertain terms of $\boldsymbol{J}$, i.e.,

$$\boldsymbol{J}_d = \mathrm{diag}(J_{xx}, J_{yy}, J_{zz}, J_{xy}\boldsymbol{I}_2, J_{xz}\boldsymbol{I}_2, J_{yz}\boldsymbol{I}_2) \tag{4.27}$$

where $\boldsymbol{I}_2$ is an identity matrix of size 2. The $\boldsymbol{J}_d$ matrix can now be associated with two placement matrices $\boldsymbol{R}_J$ and $\boldsymbol{S}_J$,

$$\boldsymbol{R}_J = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad \boldsymbol{S}_J^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

to give the factorized expression of $\boldsymbol{J}$ as follows

$$\boldsymbol{J} = \boldsymbol{R}_J \boldsymbol{J}_d \boldsymbol{S}_J \tag{4.28}$$

Remark 4.3. *The factorization* (4.28) *can be used to factorize any symmetric matrix of size* 3×3.

The inertia uncertainty can be expressed by direct multiplicative uncertainty as [38]

$$\boldsymbol{J}_d = \boldsymbol{J}_{d0}(\boldsymbol{I} + \boldsymbol{\Delta}_J) \tag{4.29}$$

where $\boldsymbol{J}_{d0}$ consists of nominal values of $\boldsymbol{J}_d$ and $\boldsymbol{\Delta}_J$ represents the considered uncertainty in the diagonal form

$$\boldsymbol{\Delta}_J = \mathrm{diag}(\Delta J_{xx}, \Delta J_{yy}, \Delta J_{zz}, \Delta J_{xy}\boldsymbol{I}_2, \Delta J_{xz}\boldsymbol{I}_2, \Delta J_{yz}\boldsymbol{I}_2) \tag{4.30}$$

with $|\Delta J_{ij}| \leq \bar{\delta}_{ij}, \forall i, j \in \{x, y, z\}$, where $0 \leq \bar{\delta}_{ij} \leq 1$ is the upper bound of the considered uncertainty level in the given axis. If $\bar{\delta}_{ij} < 1$ for any i, j couple, it is possible to reduce conservatism by introducing the following scaling

$$\boldsymbol{\Delta}_J = \boldsymbol{W}\boldsymbol{\Delta}_J^*, \qquad \boldsymbol{\Delta}_J^{*T}\boldsymbol{\Delta}_J^* \leq \boldsymbol{I} \tag{4.31}$$

where

$$\boldsymbol{W} = \mathrm{diag}(\bar{\delta}_{xx}, \bar{\delta}_{yy}, \bar{\delta}_{zz}, \bar{\delta}_{xy}\boldsymbol{I}_2, \bar{\delta}_{xz}\boldsymbol{I}_2, \bar{\delta}_{yz}\boldsymbol{I}_2)$$

In [38], the multiplicative uncertainty (4.29) was used to build a Linear Fractional Representation (LFR). In this work, the concern is about the additive uncertainty. Therefore, inserting (4.29) into (4.28) gives the inertia matrix expressed in the additive uncertainty form

$$\boldsymbol{J} = \boldsymbol{J}_0 + \boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J \tag{4.32}$$

with

$$\boldsymbol{J}_0 = \boldsymbol{R}_J \boldsymbol{J}_{d0} \boldsymbol{S}_J$$
$$\boldsymbol{R}_J^* = \boldsymbol{R}_J \boldsymbol{J}_{d0} \boldsymbol{W}$$

Since the inverse of $\boldsymbol{J}$ appears in (4.25), it is essential to express this inverse in a factorized form. Proposition 4.2 provides a method to achieve it.

Proposition 4.2 (Uncertain inertia inverse factorization)**.** *If* $\|\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\|\|\boldsymbol{S}_J\| \leq 1$*, then the inverse of the uncertain inertia matrix* (4.32) *can be expressed as*

$$\boldsymbol{J}^{-1} = \boldsymbol{J}_0^{-1} + \boldsymbol{R}_2 \boldsymbol{\Delta}_2 \boldsymbol{S}_2 \tag{4.33}$$

where $\boldsymbol{R}_2$*,* $\boldsymbol{S}_2$ *are constant matrices given by* $\boldsymbol{R}_2 = \boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\|(\boldsymbol{I} + \boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^{-1}\|$ *and* $\boldsymbol{S}_2 = \boldsymbol{S}_J\boldsymbol{J}_0^{-1}$*. Matrix* $\boldsymbol{\Delta}_2$ *satisfies* $\boldsymbol{\Delta}_2^T\boldsymbol{\Delta}_2 \leq \boldsymbol{I}$*.*

Proof. The real inertia matrix $\boldsymbol{J}$ is always invertible and symmetric, thus $\boldsymbol{J}_0$ and $\boldsymbol{J}_0 + \boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J$ are invertible and symmetric, too. Now, multiplying (4.32) with $\boldsymbol{J}_0^{-1}$ from the left, yields

$$\boldsymbol{J}_0^{-1}\boldsymbol{J} = \boldsymbol{I} + \boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J \tag{4.34}$$

and inverting both sides gives

$$\boldsymbol{J}^{-1}\boldsymbol{J}_0 = (\boldsymbol{I} + \boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J)^{-1} \tag{4.35}$$

Since $\boldsymbol{\Delta}_J^{*T}\boldsymbol{\Delta}_J^* \leq \boldsymbol{I} \Rightarrow \|\boldsymbol{\Delta}_J^*\| \leq 1$, following bound yields

$$\|\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J\| \leq \|\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\|\|\boldsymbol{\Delta}_J^*\|\|\boldsymbol{S}_J\| \leq \|\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\|\|\boldsymbol{S}_J\| \tag{4.36}$$

Thus, if $\|\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\|\|\boldsymbol{S}_J\| < 1$, then the right-hand side of (4.35) can be expressed according to Neumann series Lemma A1 (see Appendix A) as follows

$$(\boldsymbol{I} - (-\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J))^{-1} = \sum_{k=0}^{\infty}(-1)^k(\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J)^k \tag{4.37}$$

Now, pre-multiplying (4.35) by $\boldsymbol{J}_0^{-1}$ from the right and substituting (4.37) gives

$$\begin{aligned}\boldsymbol{J}^{-1} &= \sum_{k=0}^{\infty}(-1)^k(\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J)^k\boldsymbol{J}_0^{-1} \\ &= \boldsymbol{J}_0^{-1} + \sum_{k=1}^{\infty}(-1)^k(\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*\boldsymbol{S}_J)^k\boldsymbol{J}_0^{-1} = \boldsymbol{J}_0^{-1} + \boldsymbol{R}_1\boldsymbol{\Delta}_1\boldsymbol{S}_1\end{aligned} \tag{4.38}$$

where

$$\boldsymbol{R}_1 = \boldsymbol{J}_0^{-1}\boldsymbol{R}_J^* \tag{4.39}$$
$$\boldsymbol{S}_1 = \boldsymbol{S}_J\boldsymbol{J}_0^{-1} \tag{4.40}$$
$$\boldsymbol{\Delta}_1 = \boldsymbol{\Delta}_J^*(-\boldsymbol{I} + \boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^* - (\boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\boldsymbol{\Delta}_J^*)^2 + \ldots) \tag{4.41}$$

Now, it is necessary to check if $\boldsymbol{\Delta}_1^T\boldsymbol{\Delta}_1 \leq 1$. Considering the worst-case uncertainty, i.e., $\boldsymbol{\Delta}_J^* = \boldsymbol{I}$,

and inserting it in (4.41) yields to

$$\bar{\boldsymbol{\Delta}}_1 = -\boldsymbol{I} + \boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^* - (\boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^2 + \ldots = -\sum_{k=0}^{\infty}(-1)^k(\boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^k \tag{4.42}$$

which gives the upper bound of $\boldsymbol{\Delta}_1$, i.e., $\|\boldsymbol{\Delta}_1\| \leq \|\bar{\boldsymbol{\Delta}}_1\|$. According to Lemma A1, the right-hand side of (4.42) is equivalent to

$$\bar{\boldsymbol{\Delta}}_1 = -\sum_{k=0}^{\infty}(-1)^k(\boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^k = -(\boldsymbol{I} + \boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^{-1} \tag{4.43}$$

if $\|\boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\| < 1$, which is true since $\|\boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\| \leq \|\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*\|\|\boldsymbol{S}_J\| < 1$. It is obvious that $\|\bar{\boldsymbol{\Delta}}_1\| = \|(\boldsymbol{I} + \boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^{-1}\| > 1$, thus a new scaling matrix $\boldsymbol{W}_2$ must be introduced such that

$$\boldsymbol{\Delta}_1 = \boldsymbol{W}_2\boldsymbol{\Delta}_2, \qquad \boldsymbol{\Delta}_2^T\boldsymbol{\Delta}_2 \leq \boldsymbol{I} \tag{4.44}$$

where $\boldsymbol{\Delta}_2$ is unknown. One of the possible choice of $\boldsymbol{W}_2$ is to take the norm upper bound of $\boldsymbol{\Delta}_1$, i.e.,

$$\boldsymbol{W}_2 = \|\bar{\boldsymbol{\Delta}}_1\|\boldsymbol{I} = \|(\boldsymbol{I} + \boldsymbol{S}_J\boldsymbol{J}_0^{-1}\boldsymbol{R}_J^*)^{-1}\|\boldsymbol{I} \tag{4.45}$$

Then, the following holds

$$\|\boldsymbol{\Delta}_1\| = \|\boldsymbol{W}_2\boldsymbol{\Delta}_2\| = \|\bar{\boldsymbol{\Delta}}_1\|\|\boldsymbol{\Delta}_2\| \leq \|\bar{\boldsymbol{\Delta}}_1\| \;\Rightarrow\; \boldsymbol{\Delta}_2^T\boldsymbol{\Delta}_2 \leq \boldsymbol{I}$$

Inserting (4.44) into (4.38) and setting $\boldsymbol{R}_2 = \boldsymbol{R}_1\boldsymbol{W}_2$, $\boldsymbol{S}_2 = \boldsymbol{S}_1$, (4.38) yields (4.33). ■

Using proposition 4.2 with the definition of the state vector $\boldsymbol{x} = \boldsymbol{\omega}$, it can be verified, that equation (4.25) can be represented in the following nonlinear state space representation

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{\Phi}(\boldsymbol{x}(t)) + \Delta\boldsymbol{\Phi}(\boldsymbol{x}(t)) + (\boldsymbol{B} + \Delta\boldsymbol{B})\tilde{\boldsymbol{u}}_f(t) \tag{4.46}$$

$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \tag{4.47}$$

with the following assignments

$$\begin{aligned} \boldsymbol{\Phi}(\boldsymbol{x}(t)) &= -\boldsymbol{J}_0^{-1}\boldsymbol{x}(t) \times \boldsymbol{J}_0\boldsymbol{x}(t) - \boldsymbol{A}\boldsymbol{x}(t), \quad \Delta\boldsymbol{B} = \boldsymbol{R}_2\boldsymbol{\Delta}_2\boldsymbol{S}_2\boldsymbol{B}_T, \quad \boldsymbol{A} = \left.\frac{\partial\dot{\boldsymbol{x}}}{\partial\boldsymbol{x}}\right|_{(x_0,J_0)} \\ \Delta\boldsymbol{\Phi}(\boldsymbol{x}(t)) &= -\boldsymbol{J}^{-1}\boldsymbol{x}(t) \times \boldsymbol{J}\boldsymbol{x}(t) + \boldsymbol{J}_0^{-1}\boldsymbol{x}(t) \times \boldsymbol{J}_0\boldsymbol{x}(t), \quad \boldsymbol{B} = \boldsymbol{J}_0^{-1}\boldsymbol{B}_T, \quad \boldsymbol{C} = \boldsymbol{I} \end{aligned} \tag{4.48}$$

This formulation is also suitable for the NUIO theory proposed in the following section.

4.4.2 Robust Nonlinear Unknown Input Observer Design

In this section, a nonlinear unknown input observer approach for a class of uncertain Lipschitz systems is considered. The result is an observer with an $\mathcal{L}_2$ attenuation level κ from $\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}$ to the estimation error $\boldsymbol{e}$, i.e., $\|\boldsymbol{e}\|_{l2} \leq \kappa\|\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}\|_{l2}$, guaranteing asymptotic stability of the estimation error dynamics and robustness against Lipschitz nonlinear uncertainties as well as against time-varying parametric uncertainties in the input matrix. Furthermore, the estimation error dynamics is adjustable and is exactly decoupled from the considered unknown inputs. The admissible Lipschitz constant is maximized through LMI optimization.

4.4.3 Problem Statement

Consider the model given by (4.46)-(4.47) without the nonlinear uncertainty $\Delta\boldsymbol{\Phi}(\boldsymbol{x})$, but with a disturbance vector $\boldsymbol{d}$ occurring in the state equation (this will be justified later, see Section 4.4.7), i.e.,

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{\Phi}(\boldsymbol{x}(t)) + (\boldsymbol{B} + \Delta\boldsymbol{B})\boldsymbol{u}_f(t) + \boldsymbol{E}\boldsymbol{d}(t) \tag{4.49}$$

$$\boldsymbol{y}(t) = \boldsymbol{C}\boldsymbol{x}(t) \tag{4.50}$$

As usual in UIO theory, the design of the UIO parameters is done without fault consideration, i.e., $\boldsymbol{\Psi} = 0 \Rightarrow \tilde{\boldsymbol{u}}_f = \tilde{\boldsymbol{u}}$. Thus, fault sensitivity performance can only be checked "a posteriori". This usually results in some rank conditions, see for instance [60, 231].

Assumption 4.1. It is assumed that $\boldsymbol{\Phi}(\boldsymbol{x}) \in \mathbb{R}^n$ is Lipschitz in a region $\mathcal{S}$ containing the origin, i.e.,

$$\|\boldsymbol{\Phi}(\boldsymbol{x}_1) - \boldsymbol{\Phi}(\boldsymbol{x}_2)\| \leq \gamma\|\boldsymbol{x}_1 - \boldsymbol{x}_2\|, \quad \forall(\boldsymbol{x}_1, \boldsymbol{x}_2) \in \mathcal{S}$$

where $\gamma > 0$ stands for the Lipschitz constant. If $\mathcal{S} = \mathbb{R}^n$, $\boldsymbol{\Phi}$ is globally Lipschitz. Otherwise, it is locally Lipschitz.

Assumption 4.2. It is assumed that $\boldsymbol{E}$ is of full column rank and that the system satisfies

$$\text{rank}(\boldsymbol{C}\boldsymbol{E}) = \text{rank}(\boldsymbol{E}).$$

Remark 4.4. *Assumption 4.1 is reasonable in our case, since $\boldsymbol{\Phi}(\boldsymbol{x}) = \boldsymbol{\Phi}(\boldsymbol{\omega})$ in (4.46) is continuously differentiable on $\mathbb{R}^3$ and thus, it is locally Lipschitz, see [7]. This means that the angular velocity shall be bounded in magnitude which is a reasonable assumption from a practical point of view, too. Assumption 4.2 can be done without loss of generality, see Remark 3.7 if necessary.*

Under assumptions 4.1-4.2, the goal turns out to be the design of the following NUIO

$$\dot{\boldsymbol{z}}(t) = \boldsymbol{N}\boldsymbol{z}(t) + \boldsymbol{G}\tilde{\boldsymbol{u}}(t) + \boldsymbol{L}\boldsymbol{y}(t) + \boldsymbol{M}\boldsymbol{\Phi}\left(\hat{\boldsymbol{x}}(t)\right) \tag{4.51}$$

$$\hat{\boldsymbol{x}}(t) = \boldsymbol{z}(t) + \boldsymbol{H}\boldsymbol{y}(t) \tag{4.52}$$

in such a way that $\hat{\boldsymbol{x}}$ lends robustness against the uncertainties $\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}$ and is decoupled from the unknown inputs $\boldsymbol{d}$. In (4.51)–(4.52), $\hat{\boldsymbol{x}} \in \mathbb{R}^n$ stands for the estimate of $\boldsymbol{x}$ and $\boldsymbol{z} \in \mathbb{R}^n$ is an auxiliary signal.

To proceed, define the estimation error as

$$\boldsymbol{e}(t) = \boldsymbol{x}(t) - \hat{\boldsymbol{x}}(t) \tag{4.53}$$

For notation simplicity let

$$\boldsymbol{\Phi}(\hat{\boldsymbol{x}}(t)) = \hat{\boldsymbol{\Phi}}, \qquad \boldsymbol{\Phi}(\boldsymbol{x}(t)) = \boldsymbol{\Phi} \tag{4.54}$$

The estimation error dynamics is governed by (omitting the time dependency here)

$$\begin{aligned}\dot{\boldsymbol{e}} = \boldsymbol{N}\boldsymbol{e} + ((\boldsymbol{I} - \boldsymbol{H}\boldsymbol{C})\boldsymbol{A} + \boldsymbol{N}(\boldsymbol{I} - \boldsymbol{H}\boldsymbol{C}) - \boldsymbol{L}\boldsymbol{C})\boldsymbol{x} + (\boldsymbol{I} - \boldsymbol{H}\boldsymbol{C})\Delta\boldsymbol{B}\tilde{\boldsymbol{u}} \\ +((\boldsymbol{I} - \boldsymbol{H}\boldsymbol{C})\boldsymbol{B} - \boldsymbol{G})\tilde{\boldsymbol{u}} + (\boldsymbol{I} - \boldsymbol{H}\boldsymbol{C})\boldsymbol{\Phi} - \boldsymbol{M}\hat{\boldsymbol{\Phi}} + (\boldsymbol{I} - \boldsymbol{H}\boldsymbol{C})\boldsymbol{E}\boldsymbol{d}\end{aligned} \tag{4.55}$$

To make the error dynamics (4.55) independent of the state $\boldsymbol{x}$, of the unknown input $\boldsymbol{d}$, and of

$((\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{B}-\boldsymbol{G})\tilde{\boldsymbol{u}}$, respectively, the following must hold

$$\boldsymbol{N} = \boldsymbol{MA} - \boldsymbol{KC}, \tag{4.56}$$

$$\boldsymbol{L} = \boldsymbol{K}(\boldsymbol{I}-\boldsymbol{CH}) + \boldsymbol{MAH}, \tag{4.57}$$

$$\boldsymbol{M} = \boldsymbol{I} - \boldsymbol{HC}, \tag{4.58}$$

$$\boldsymbol{G} = \boldsymbol{MB} \tag{4.59}$$

$$(\boldsymbol{I}-\boldsymbol{HC})\boldsymbol{E} = \boldsymbol{0} \tag{4.60}$$

It can be verified that (4.55) reduces to

$$\dot{\boldsymbol{e}} = \boldsymbol{Ne} + \boldsymbol{M}(\boldsymbol{\Phi} - \hat{\boldsymbol{\Phi}}) + \boldsymbol{M}\Delta\boldsymbol{B}\tilde{\boldsymbol{u}} \tag{4.61}$$

Equation (4.60) can be rewritten as

$$\boldsymbol{HCE} = \boldsymbol{E} \tag{4.62}$$

and the necessary condition for this equation to have a solution is that Assumption 4.2 is satisfied. The general solution of (4.62) can be written according to [55]

$$\boldsymbol{H} = \boldsymbol{U} + \boldsymbol{YV} \tag{4.63}$$

where $\boldsymbol{Y}$ must be chosen such that it does not cause rank deficiency of $\boldsymbol{H}$. Matrices $\boldsymbol{U}$ and $\boldsymbol{V}$ are given by

$$\boldsymbol{U} = \boldsymbol{E}(\boldsymbol{CE})^{\dagger}, \quad \boldsymbol{V} = \boldsymbol{I} - (\boldsymbol{CE})(\boldsymbol{CE})^{\dagger} \tag{4.64}$$

where $(\boldsymbol{CE})^{\dagger}$ is the generalized pseudoinverse of the matrix $\boldsymbol{CE}$.

The aim is now to design the parameters $\boldsymbol{K}$ and $\boldsymbol{Y}$ in such a way that the estimation error dynamics (4.61) is asymptotically stable with maximum admissible Lipschitz constant γ^* and such that the $\mathcal{L}_2$ gain from $\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}$ to the estimation error $\boldsymbol{e}$ is bounded by

$$\frac{\|\boldsymbol{e}\|_{l2}}{\|\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}\|_{l2}} \leq \kappa, \quad \forall\tilde{\boldsymbol{u}} \in \mathcal{L}_2[0,\infty),\ \|\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}\|_{l2} \neq 0 \tag{4.65}$$

for a given $\kappa > 0$.

4.4.4 LMI-based Synthesis

The following theorem provides a LMI-based design method for the NUIO.

Theorem 4.1. *Consider the (Lipschitz) nonlinear system* (4.49)-(4.50). *The NUIO* (4.51)-(4.52) *is asymptotically stable with maximum admissible Lipschitz constant* γ^* *and the* $\mathcal{L}_2$ *gain from* $\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}$ *to* $\boldsymbol{e}$ *is bounded by* $\kappa > 0$, *if there exists a positive definite matrix* $\boldsymbol{P} = \boldsymbol{P}^T > 0$ *and matrices* $\bar{\boldsymbol{K}}$, $\bar{\boldsymbol{Y}}$ *as solutions of the following optimization problem:*

$$\max_{P,\bar{K},\bar{Y}} \xi \tag{4.66}$$

$$s.t. \begin{bmatrix} \boldsymbol{\Psi}_{11}+\boldsymbol{\Gamma}_{11} & \boldsymbol{\Omega}_{12} & \boldsymbol{\Omega}_{13} & \boldsymbol{0} & \boldsymbol{0} \\ * & -\boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ * & * & -\boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \\ * & * & * & -\kappa^2\boldsymbol{I} & \boldsymbol{S}_2\boldsymbol{B_T} \\ * & * & * & * & -\boldsymbol{I} \end{bmatrix} < 0, \quad \begin{bmatrix} \xi & \gamma \\ * & 1 \end{bmatrix} \geq 0 \tag{4.67}$$

where

$$\boldsymbol{\Psi}_{11} = ((\boldsymbol{I}-\boldsymbol{UC})\boldsymbol{A})^T\boldsymbol{P} + \boldsymbol{P}(\boldsymbol{I}-\boldsymbol{UC})\boldsymbol{A} + (1+\xi)\boldsymbol{I} \tag{4.68}$$

$$\boldsymbol{\Gamma}_{11} = -(\boldsymbol{VCA})^T\bar{\boldsymbol{Y}}^T - \bar{\boldsymbol{Y}}\boldsymbol{VCA} - \boldsymbol{C}^T\bar{\boldsymbol{K}}^T - \bar{\boldsymbol{K}}\boldsymbol{C} \tag{4.69}$$

$$\boldsymbol{\Omega}_{12} = \boldsymbol{P}(\boldsymbol{I}-\boldsymbol{UC}) - \bar{\boldsymbol{Y}}\boldsymbol{VC} \tag{4.70}$$

$$\boldsymbol{\Omega}_{13} = \boldsymbol{P}(\boldsymbol{I}-\boldsymbol{UC})\boldsymbol{R}_2 - \bar{\boldsymbol{Y}}\boldsymbol{VCR}_2 \tag{4.71}$$

$$\tag{4.72}$$

Once the problem is solved, then

$$\boldsymbol{K} = \boldsymbol{P}^{-1}\bar{\boldsymbol{K}} \tag{4.73}$$

$$\boldsymbol{Y} = \boldsymbol{P}^{-1}\bar{\boldsymbol{Y}} \tag{4.74}$$

$$\gamma^* = \sqrt{\xi} \tag{4.75}$$

Proof. Assume that $\boldsymbol{H}$ is chosen such that (4.60) holds. Under the assumption that $\boldsymbol{\Delta B} = \boldsymbol{R}_2\boldsymbol{\Delta}_2\boldsymbol{S}_2\boldsymbol{B}_T$ with $\boldsymbol{\Delta}_2^T\boldsymbol{\Delta}_2 \leq \boldsymbol{I}$, the error dynamics of the NUIO (4.61) can be rewritten as

$$\dot{\boldsymbol{e}} = \boldsymbol{Ne} + \boldsymbol{M}(\boldsymbol{\Phi}-\hat{\boldsymbol{\Phi}}) + \boldsymbol{MR}_2\boldsymbol{\Delta}_2\boldsymbol{S}_2\boldsymbol{B}_T\tilde{\boldsymbol{u}} \tag{4.76}$$

Considering a quadratic Lyapunov function $V(t) = \boldsymbol{e}(t)^T\boldsymbol{Pe}(t)$, where $\boldsymbol{P} = \boldsymbol{P}^T > 0$. The time derivative of $V(t)$ along the trajectory of (4.76) is given by

$$\dot{V} = \boldsymbol{e}^T(\boldsymbol{N}^T\boldsymbol{P}+\boldsymbol{PN})\boldsymbol{e} + 2\boldsymbol{e}^T\boldsymbol{PM}(\boldsymbol{\Phi}-\hat{\boldsymbol{\Phi}}) + 2\boldsymbol{e}^T\boldsymbol{PMR}_2\boldsymbol{\Delta}_2\boldsymbol{S}_2\boldsymbol{B}_T\tilde{\boldsymbol{u}} \tag{4.77}$$

Using the Lipschitz condition stated in Assumption 4.1 and Lemma A4 (see Appendix A) with $\epsilon = 1$, it follows that

$$2\boldsymbol{e}^T\boldsymbol{PM}(\hat{\boldsymbol{\Phi}}-\boldsymbol{\Phi}) \leq 2\gamma\|\boldsymbol{e}^T\boldsymbol{PM}\|\|e\| \leq \boldsymbol{e}^T\boldsymbol{PMM}^T\boldsymbol{Pe} + \gamma^2\boldsymbol{e}^T\boldsymbol{e}$$
$$2\boldsymbol{e}^T\boldsymbol{PMR}_2\boldsymbol{\Delta}_2\boldsymbol{S}_2\boldsymbol{B}_T\tilde{\boldsymbol{u}} \leq \boldsymbol{e}^T\boldsymbol{PMR}_2\boldsymbol{R}_2^T\boldsymbol{M}^T\boldsymbol{Pe} + \tilde{\boldsymbol{u}}^T(\boldsymbol{S}_2\boldsymbol{B}_T)^T\boldsymbol{S}_2\boldsymbol{B}_T\tilde{\boldsymbol{u}}$$

and (4.77) can be bounded as follows

$$\dot{V} \leq \boldsymbol{e}^T(\boldsymbol{N}^T\boldsymbol{P}+\boldsymbol{PN} + \boldsymbol{PM}(\boldsymbol{I}+\boldsymbol{R}_2\boldsymbol{R}_2^T)\boldsymbol{M}^T\boldsymbol{P} + \gamma^2\boldsymbol{I})\boldsymbol{e} + \tilde{\boldsymbol{u}}^T(\boldsymbol{S}_2\boldsymbol{B}_T)^T\boldsymbol{S}_2\boldsymbol{B}_T\tilde{\boldsymbol{u}} \tag{4.78}$$

If the $\mathcal{H}_\infty$ performance criteria is considered

$$\min_{\kappa} : \int_0^{T_f} \boldsymbol{e}^T(t)\boldsymbol{e}(t)dt \leq \kappa^2 \int_0^{T_f} \tilde{\boldsymbol{u}}^T(t)\tilde{\boldsymbol{u}}(t)dt \quad \forall T_f \geq 0 \tag{4.79}$$

then it is straightforward to verify that the $\mathcal{L}_2$ gain from $\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}$ to $\boldsymbol{e}$ is bounded by $\kappa > 0$ if and only if

$$\boldsymbol{e}^T\boldsymbol{e} - \kappa^2\tilde{\boldsymbol{u}}^T\tilde{\boldsymbol{u}} + \dot{V} = \begin{bmatrix} \boldsymbol{e}^T & \tilde{\boldsymbol{u}}^T \end{bmatrix} \begin{bmatrix} \boldsymbol{\Psi}_1 & \boldsymbol{0} \\ * & \boldsymbol{\Psi}_2 \end{bmatrix} \begin{bmatrix} \boldsymbol{e} \\ \tilde{\boldsymbol{u}} \end{bmatrix} < 0 \tag{4.80}$$

where

$$\boldsymbol{\Psi}_1 = \boldsymbol{N}^T\boldsymbol{P} + \boldsymbol{P}\boldsymbol{N} + (1+\gamma^2)\boldsymbol{I} + \boldsymbol{P}\boldsymbol{M}(\boldsymbol{I} + \boldsymbol{R}_2\boldsymbol{R}_2^T)\boldsymbol{M}^T\boldsymbol{P}$$
$$\boldsymbol{\Psi}_2 = (\boldsymbol{S}_2\boldsymbol{B}_T)^T\boldsymbol{S}_2\boldsymbol{B}_T - \kappa^2\boldsymbol{I}$$

The following LMI

$$\begin{bmatrix} \boldsymbol{\Psi}_1 & \boldsymbol{0} \\ * & \boldsymbol{\Psi}_2 \end{bmatrix} < 0 \tag{4.81}$$

should hold to satisfy (4.80). Then, by virtue of the Schur's complement Lemma A3, (4.81) is equivalent to

$$\begin{bmatrix} \boldsymbol{N}^T\boldsymbol{P} + \boldsymbol{P}\boldsymbol{N} + (1+\gamma^2)\boldsymbol{I} & \boldsymbol{P}\boldsymbol{M} & \boldsymbol{P}\boldsymbol{M}\boldsymbol{R}_2 & \boldsymbol{0} & \boldsymbol{0} \\ * & -\boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ * & * & -\boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \\ * & * & * & -\kappa^2\boldsymbol{I} & \boldsymbol{S}_2\boldsymbol{B}_T \\ * & * & * & * & -\boldsymbol{I} \end{bmatrix} < 0 \tag{4.82}$$

It can be seen that there is no systematic way to obtain the observer parameters directly from (4.82) due to coupled terms. To reformulate (4.82) as an LMI, we substitute $\boldsymbol{H}$ given by (4.63), and use the following assignments $\bar{\boldsymbol{Y}} = \boldsymbol{P}\boldsymbol{Y}$, $\bar{\boldsymbol{K}} = \boldsymbol{P}\boldsymbol{K}$ and $\xi = \gamma^2$. Additionally, it is desired to achieve the maximum possible Lipschitz constant γ^* and simultaneously to respect the constraint $\gamma^* \geq \gamma$. This constraint can be rewritten by defining a new variable $\xi = (\gamma^*)^2$ as

$$\xi - \gamma^2 \geq 0 \tag{4.83}$$

Then, using the Schur's complement, (4.67) follows. It is then obvious that maximizing ξ is equivalent to maximizing γ^*. This concludes the proof. ■

4.4.5 Robustness Against Nonlinear Uncertainty

Consider here the fully uncertain attitude dynamics given by (4.46). Recalling the nonlinear terms, i.e.,

$$\boldsymbol{\Phi}_\Delta(\boldsymbol{x}) = \boldsymbol{\Phi}(\boldsymbol{x}) + \Delta\boldsymbol{\Phi}(\boldsymbol{x}) \tag{4.84}$$

where $\boldsymbol{\Phi}_\Delta$ is the uncertain nonlinear function and $\Delta\boldsymbol{\Phi}$ is the unknown part of $\boldsymbol{\Phi}_\Delta$. Suppose that

$$\|\Delta\boldsymbol{\Phi}(\boldsymbol{x}_1) - \Delta\boldsymbol{\Phi}(\boldsymbol{x}_2)\| \leq {}_\Delta\gamma\|\boldsymbol{x}_1 - \boldsymbol{x}_2\|, \;\; \forall(\boldsymbol{x}_1, \boldsymbol{x_2}) \in \mathcal{S} \tag{4.85}$$

Proposition 4.3 (Abbaszadeh and Marquez [1])**.** *Assumming that the actual Lipschitz constant of the system is γ and the maximum admissible Lipschitz constant achieved by Theorem 4.1 is γ^*. Then, the observer designed based on Theorem 4.1, can tolerate any additive Lipschitz nonlinear uncertainty $\Delta\boldsymbol{\Phi}(\boldsymbol{x})$ with Lipschitz constant less than or equal to $\gamma^* - \gamma$.*

Proof. Based on Schwartz inequality, it follows

$$\|\boldsymbol{\Phi}_\Delta(\boldsymbol{x}_1) - \boldsymbol{\Phi}_\Delta(\boldsymbol{x}_2)\| \leq$$
$$\|\boldsymbol{\Phi}(\boldsymbol{x}_1) - \boldsymbol{\Phi}(\boldsymbol{x}_2)\| + \|\Delta\boldsymbol{\Phi}(\boldsymbol{x}_1) - \Delta\boldsymbol{\Phi}(\boldsymbol{x}_2)\| \leq (\gamma + {}_\Delta\gamma)\|\boldsymbol{x}_1 - \boldsymbol{x}_2\|$$

According to Theorem 4.1, $\boldsymbol{\Phi}_\Delta(\boldsymbol{x})$ can be any Lipschitz nonlinear function with Lipschitz constant less than or equal to γ^*,

$$\|\boldsymbol{\Phi}_\Delta(\boldsymbol{x}_1) - \boldsymbol{\Phi}_\Delta(\boldsymbol{x}_2)\| \leq \gamma^* \|\boldsymbol{x}_1 - \boldsymbol{x}_2\|, \;\; \forall(\boldsymbol{x}_1, \boldsymbol{x_2}) \in \mathcal{S}$$

so there must be $(\gamma + {}_\Delta\gamma) \leq \gamma^* \rightarrow {}_\Delta\gamma \leq \gamma^* - \gamma$. ■

For any continuously differentiable function $\boldsymbol{\Delta\Phi}$ the following holds

$$\|\Delta\boldsymbol{\Phi}(\boldsymbol{x}_1) - \Delta\boldsymbol{\Phi}(\boldsymbol{x}_2)\| \leq \|\frac{\partial\Delta\boldsymbol{\Phi}}{\partial\boldsymbol{x}}(\boldsymbol{x}_1 - \boldsymbol{x}_2)\|, \;\; \forall(\boldsymbol{x}_1, \boldsymbol{x_2}) \in \mathcal{S}$$

where $\partial\Delta\boldsymbol{\Phi}/\partial\boldsymbol{x}$ is the Jacobian matrix. Therefore, according to [1], $\boldsymbol{\Delta\Phi}$ can be any additive uncertainty with $\|\partial\Delta\boldsymbol{\Phi}/\partial\boldsymbol{x}\| \leq \gamma^* - \gamma$.

4.4.6 NUIO Dynamics Adjustment

The maximization of the admissible Lipschitz constant γ^* may result in unsatisfactory dynamical behaviour of the state estimation error. To overcome this problem, the $\mathcal{D}$-stability concept proposed by Chilali and Gahinet [45] can be used jointly with Theorem 4.1, thanks to the LMI formulation (4.67). First, the definition of an LMI region is recalled here and some results on the pole placement LMI constraints are introduced in order to prove the proposed proposition to come.

Definition 4.1 (LMI region [45])**.** A subset $\mathcal{D}$ of the complex plane is called an LMI region if there exist two symmetric matrices $\boldsymbol{\alpha} = [\alpha_{kl}] \in \mathbb{R}^{p\times p}$ and $\boldsymbol{\beta} = [\beta_{kl}] \in \mathbb{R}^{p\times p}$, such that

$$\mathcal{D} = \{z \in \mathbb{C} : \boldsymbol{f}_{\mathcal{D}}(z) = \boldsymbol{\alpha} + \boldsymbol{\beta}z + \boldsymbol{\beta}^T\bar{z} < 0\} \tag{4.86}$$

where $\boldsymbol{f}_{\mathcal{D}}(z)$ is called the characteristic function of $\mathcal{D}$.

Theorem 4.2 (Chilali and Gahinet [45])**.** *Eigenvalues of a real matrix $\boldsymbol{X}$ lie in $\mathcal{D}$, if and only if there exists a symmetric positive definite matrix $\boldsymbol{P} > 0$, such that*

$$\boldsymbol{M}_{\mathcal{D}}(\boldsymbol{X}, \boldsymbol{P}) = \boldsymbol{\alpha} \otimes \boldsymbol{P} + \boldsymbol{\beta} \otimes (\boldsymbol{XP}) + \boldsymbol{\beta}^T \otimes (\boldsymbol{XP})^T < 0 \tag{4.87}$$

where $\otimes$ stands for the Kronecker product of two matrices.

Proof. The proof can be found in [45]. ■

Corollary 4.1 (Chilali and Gahinet [45])**.** *Given two LMI regions $\mathcal{D}_1$ and $\mathcal{D}_2$, the eigenvalues of a matrix $\boldsymbol{X}$ lie in $\mathcal{D}_1 \cap \mathcal{D}_2$ if and only if there exists a positive definite matrix $\boldsymbol{P}$ such that $\boldsymbol{M}_{\mathcal{D}_1}(\boldsymbol{X}, \boldsymbol{P}) < 0$ and $\boldsymbol{M}_{\mathcal{D}_2}(\boldsymbol{X}, \boldsymbol{P}) < 0$.*

In Theorem 4.1, the NUIO gain matrix $\boldsymbol{N}$, which controls the dynamical behaviour of the state estimation error, directly depends on the LMI variables $\boldsymbol{P}$, $\bar{\boldsymbol{K}}$ and $\bar{\boldsymbol{Y}}$, thus offering extra degree of freedom to place the eigenvalues of $\boldsymbol{N}$ in a prescribed region $\mathcal{D}$.

Proposition 4.4. *Consider the NUIO design based on Theorem 4.1. If there exists a common Lyapunov matrix $\boldsymbol{P} = \boldsymbol{P}^T > 0$ and matrices $\bar{\boldsymbol{K}}$, $\bar{\boldsymbol{Y}}$ such that the LMI optimization problem*

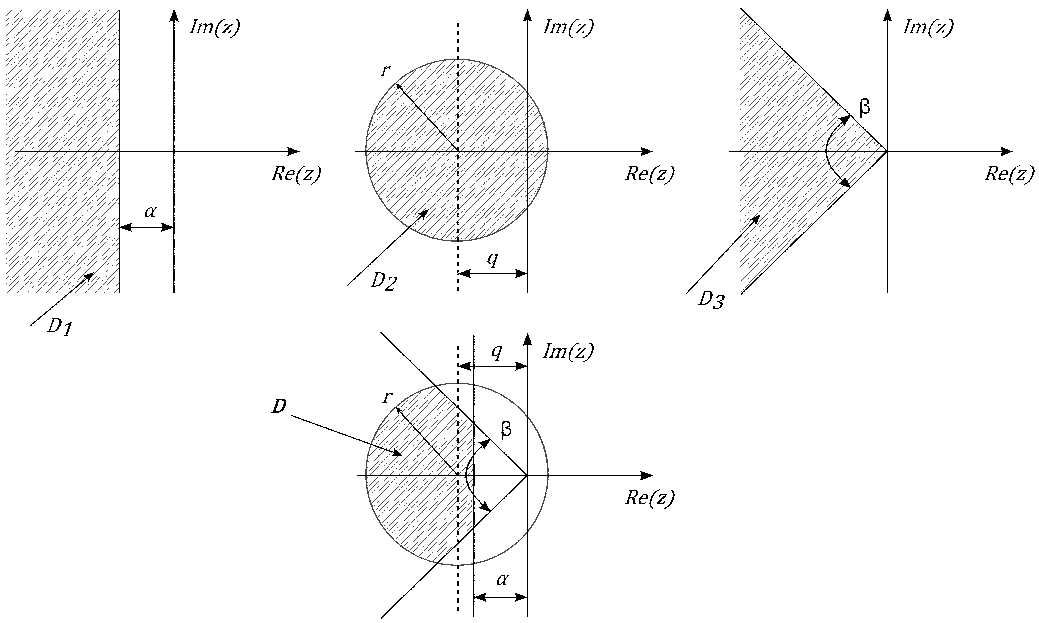


Figure 4.4 – LMI Region $\mathcal{D}(\alpha, q, r, \beta) = \mathcal{D}_1 \cap \mathcal{D}_2 \cap \mathcal{D}_3$

given in Theorem 4.1 has a solution while the set of n LMIs

$$\begin{aligned} &\boldsymbol{\alpha}_k \otimes \boldsymbol{P} + \boldsymbol{\beta}_k \otimes (\boldsymbol{A}^T\boldsymbol{P} - (\boldsymbol{UCA})^T\boldsymbol{P} - (\bar{\boldsymbol{Y}}\boldsymbol{VCA})^T - (\bar{\boldsymbol{K}}\boldsymbol{C})^T) + \\ &\boldsymbol{\beta}_k^T \otimes (\boldsymbol{PA} - \boldsymbol{P}(\boldsymbol{UCA}) - \bar{\boldsymbol{Y}}\boldsymbol{VCA} - \bar{\boldsymbol{K}}\boldsymbol{C}) < 0, \quad k = 1, 2, \ldots, n \end{aligned} \tag{4.88}$$

is simultaneously satisfied, then all eigenvalues of the matrix $\boldsymbol{N}$ will be assigned into a prescribed LMI region $\mathcal{D} = \cap_{k=1}^{n} \mathcal{D}_k$. In this expression, $\boldsymbol{\alpha}_k$ and $\boldsymbol{\beta}_k$ are matrices of appropriate dimension defining each region $\mathcal{D}_k$.

Proof. Substituting (4.58),(4.63),(4.73) and (4.74) into (4.56) and transposing it yields

$$\boldsymbol{N}^T = \boldsymbol{A}^T - (\boldsymbol{UCA})^T - (\bar{\boldsymbol{Y}}\boldsymbol{VCA})^T\boldsymbol{P}^{-1} - (\bar{\boldsymbol{K}}\boldsymbol{C})^T\boldsymbol{P}^{-1} \tag{4.89}$$

If the LMI conditions (4.67) and (4.88) are satisfied at the same time, then the proof of Proposition 4.4 directly follows from Theorem 4.2, from Corollary 4.1, and from the fact that eigenvalues of any square matrix are equal to eigenvalues of its transpose, i.e., $\boldsymbol{\Lambda}(\boldsymbol{N}) = \boldsymbol{\Lambda}(\boldsymbol{N}^T)$. ■

Remark 4.5. *In Proposition 4.4, the use of $\boldsymbol{N}^T$ instead of $\boldsymbol{N}$ was motivated by elimination possibility of $\boldsymbol{P}^{-1}$ from* (4.89)*. The product $\boldsymbol{N}^T\boldsymbol{P}$ in* (4.87) *thus yields: $\boldsymbol{N}^T\boldsymbol{P} = \boldsymbol{A}^T\boldsymbol{P} - (\boldsymbol{UCA})^T\boldsymbol{P} - (\bar{\boldsymbol{Y}}\boldsymbol{VCA})^T - (\bar{\boldsymbol{K}}\boldsymbol{C})^T$.*

To modify the NUIO dynamics, results related to Proposition 4.4 are used. Here, the intersection of three elementary LMI regions $\mathcal{D}_k, k = 1, 2, 3$ are considered, which restrict the eigenvalues of $\boldsymbol{N}$ in the region $\mathcal{D} = \mathcal{D}_1 \cap \mathcal{D}_2 \cap \mathcal{D}_3$. This region is illustrated in Figure 4.4 and represented by the following LMIs:

- Left-half plane delimited by a vertical line $-\alpha$, with $\alpha > 0$

$$\boldsymbol{M}_{\mathcal{D}_1}(\boldsymbol{N}^T, \boldsymbol{P}) = 2\alpha\boldsymbol{P} + \boldsymbol{N}^T\boldsymbol{P} + \boldsymbol{PN} < 0 \tag{4.90}$$

- Disk with center at $(-q, 0)$ and radius r

$$\boldsymbol{M}_{\mathcal{D}_2}(\boldsymbol{N}^T, \boldsymbol{P}) = \begin{pmatrix} -r\boldsymbol{P} & q\boldsymbol{P} + \boldsymbol{N}^T\boldsymbol{P} \\ * & -r\boldsymbol{P} \end{pmatrix} < 0 \tag{4.91}$$

- Conic region with center at the origin and with inner angle $0 < \beta < \pi/2$ pointing left

$$\boldsymbol{M}_{\mathcal{D}_3}(\boldsymbol{N}^T, \boldsymbol{P}) = \begin{pmatrix} \sin\beta(\boldsymbol{N}^T\boldsymbol{P} + \boldsymbol{P}\boldsymbol{N}) & \cos\beta(\boldsymbol{N}^T\boldsymbol{P} - \boldsymbol{P}\boldsymbol{N}) \\ * & \sin\beta(\boldsymbol{N}^T\boldsymbol{P} + \boldsymbol{P}\boldsymbol{N}) \end{pmatrix} < 0 \tag{4.92}$$

The four degrees of freedom (α, q, r, β), used to determine $\mathcal{D}$, allow us to fix the desired region of all the eigenvalues of $\boldsymbol{N}$, i.e., $\boldsymbol{\Lambda}(\boldsymbol{N}) \in \mathcal{D}(\alpha, q, r, \beta)$.

4.4.7 Comments on NUIO Implementation and Computational Issues

For each thruster group $\mathcal{S}_{Tk}, k = 1, ..., 5$ (see (4.1) for definition), a dedicated NUIO is designed based on Algorithm 2. The Lipschitz constant γ for $\boldsymbol{\Phi}(\boldsymbol{\omega})$ is computed using a constrained optimization algorithm over the set $\mathcal{S}_\omega = \{\boldsymbol{\omega} \in \mathbb{R}^3 : |\omega_k| \leq \bar{\omega},\ k = 1, 2, 3\}$, where $\bar{\omega}$ is the upper bound of the angular velocity for each axis. The LMI region assignment approach given in Proposition 4.4 is considered to adjust adequately the dynamics of the NUIOs. In other words, the four LMI parameters (α, q, r, β) have to be chosen carefully such that the observer error dynamics reacts quick enough to any type of thruster fault, allowing early distinction among the healthy/faulty thruster groups $\mathcal{S}_{Tk}, k = 1, ..., 5$ (see the following section about the proposed thruster group isolation strategy).

Algorithm 2 Design of the bank of 5 NUIOs

```
Compute γ for Φ(ω) over S_ω and choose the attenuation level κ;
for k = 1 to 5 do
    B*_k = [b*_1, ..., b*_12] where b*_i = J_0^{-1} b_Ti, ∀i ∈ S_all \ S_Tk and b*_i = 0, ∀i ∈ S_Tk;
    Set E ≜ J_0^{-1} b_Ti for any arbitrary i ∈ S_Tk and B ≜ B*_k;
    Compute U and V according to (4.64);
    Prescribe the desired dynamics using D(α, q, r, β);
    Solve the optimisation problem (4.66) under LMI constraints (4.67) and (4.88)
    Then K = P^{-1} K̄, Y = P^{-1} Ȳ and γ*_k ≜ √ξ̄;
    Using K and Y, gains for the k^th NUIO are given by (4.56)-(4.59) and (4.63);
end for
```

The kth NUIO is such that it can fully estimate the angular velocity $\boldsymbol{\omega}$ with all control inputs but those associated with $\mathcal{S}_{Tk}$, i.e., with $\tilde{\boldsymbol{u}}_i, \forall i \in \mathcal{S}_{all} \backslash \mathcal{S}_{Tk}$. On the other hand, $\boldsymbol{d}$ in equation (4.49), stays for the control inputs associated with $\mathcal{S}_{Tk}$ (i.e., $\tilde{\boldsymbol{u}}_i, \forall i \in \mathcal{S}_{Tk}$). As a result, the NUIO dedicated to the group $\mathcal{S}_{Tk}$ shall not be affected by faults occurring in the thrusters belonging to $\mathcal{S}_{Tk}$ due to the decoupling property, while all the other NUIOs will be (are expected to be, to be more precise, since the design of the NUIOs are done without fault sensitivity specifications, see [131, 133, 134] for discussion about guaranteed sensitivity performances).

It is important to note that $\boldsymbol{d}$ can be *exactly decoupled* only if the columns of $\Delta\boldsymbol{B}$ related to $\boldsymbol{d}$ are zero. If this is not the case, only the known directions, i.e., $\boldsymbol{b}_i^* = \boldsymbol{J}_0^{-1}\boldsymbol{b}_{Ti}$, $i \in \mathcal{S}_{Tk}$, can be exactly decoupled, while the uncertain columns $\Delta\boldsymbol{b}_i^*$, $i \in \mathcal{S}_{Tk}$ (columns of $\Delta\boldsymbol{B}$ associated with

$\mathcal{S}_{Tk}$) are attenuated in $\mathcal{L}_2$ sense (with upper bound κ) since the entire $\Delta\boldsymbol{B}$ matrix is considered in (4.65). Furthermore, if a constant γ^* linked to a given NUIO verifies $\gamma^* > \gamma$, then the associated observer tolerates an additional nonlinear uncertainty in $\boldsymbol{\Phi}_\Delta(\boldsymbol{\omega})$, see discussion in Section 4.4.5.

Note, that the all observers estimate only the angular rate $\boldsymbol{\omega}$ of the chaser. Therefore, the computational burden is reduced since there is no need to process the entire state vector (i.e., the linear position/velocity and the attitude in addition). For real-time reasons, the bank of 5 NUIOs is triggered only when the decision signal $\varrho^{J_{th}}$ (see (4.22)) indicates the fault occurrence, i.e., when $\varrho^{J_{th}}(t) = 1$ for $t \geq t_d$. Even if only $\boldsymbol{\omega}$ is estimated, keeping the NUIOs switched off before the fault is detected seems to be a good strategy, concerning the nonlinear nature of the observer.

4.4.8 Thruster Group Isolation Logic - First Stage

It is obvious that, in case of (small) truster faults, the spacecraft attitude dynamics is more likely prone to dynamic deviations than the translation one. This gives the motivation to derive the first isolation rule using the angular velocity measurement rather than the one obtained from the LIDAR device. On the other hand, due to the fact that some thrusters produce exactly the same or very similar torques, it is very hard to obtain a global isolation strategy based exclusively on angular velocity measurements. Therefore, the second isolation rule of the proposed (global) isolation strategy uses the information about the position dynamics contained in the fault detector's residual. This chronology of isolation steps gives to the fault an extra time to propagate into the translation dynamics.

To proceed, let $\mathcal{S}_G = \{1, 2, ...5\}$ be the set of all the thruster group indices linked with $\mathcal{S}_{T1}, \ldots, \mathcal{S}_{T5}$. Each observer is initialized with the (known) measurement at detection time t_d, i.e., $\hat{\boldsymbol{\omega}}_k(t_d) = \boldsymbol{\omega}(t_d)$, $\forall k \in \mathcal{S}_G$. By this, all observers have a zero initial estimation error. Hence, the observer initial convergence (transient phase) problem is avoided. Defining the angular velocity estimation error $\boldsymbol{e}_k$ associated with the kth NUIO as

$$\boldsymbol{e}_k(t) = \hat{\boldsymbol{\omega}}_k(t) - \boldsymbol{\omega}(t) \tag{4.93}$$

then, it seems obvious, that the observer with the minimum estimation error $\boldsymbol{e}_k$ (in some norm sense) should reveal that the fault occurred in the associated thruster group $\mathcal{S}_{Tk}$. Such property provides an efficient isolation rule that can be written according to

$$\sigma_g(t) = \arg\min_k \|\boldsymbol{e}_k(t)\|, \quad t \geq t_d \tag{4.94}$$

where $\sigma_g(t) : \mathbb{R}^+ \to \mathcal{S}_G$ represents the identified faulty thruster group index at time "t".

To avoid initial transition phenomena and to ensure robustness against noise, a confirmation time window, $\delta_g > 0$, is introduced, i.e.,

$$t_g = \arg\inf_{t \geq t_d + \delta_g} \{\sigma_g(t) = \sigma_g(\vartheta), \forall \vartheta \in (t - \delta_g, t]\} \tag{4.95}$$

where t_g is the isolation time of the faulty thruster group. For notation simplicity, let $j = \sigma_g(t_g)$.

At this isolation stage, in the ideal case, the minimum time $(t_d - t_f) + \delta_g$ has elapsed from the true fault occurrence time, i.e., $t = t_f$, thus allowing additional time for the fault to induce observable dynamic deviation in the translation dynamics that is contained, e.g., in the fault detector's residual $\boldsymbol{r}$ given by (4.20). Therefore, as soon as the faulty thruster group index "j" is confirmed, the faulty thruster can be uniquely isolated by simply examining the degree of alignment between $\boldsymbol{r}$ and the fixed force vector directions $\boldsymbol{b}_{Fk}$, $k \in \mathcal{S}_{Tj}$ (see (2.52) for definition of $\boldsymbol{b}_{Fk}$) under the assumption that the fault type is known. This is the purpose of the next section.

Remark 4.6. *It is assumed that the time-varying delay has no big effect on the isolation performance. Therefore, $\tau(t)$ is not considered in* (4.25)*. Nevertheless, the isolation process is triggered by the decision test $\varrho^{J_{th}}(t)$, which already has enhanced robustness against $\tau(t)$.*

4.4.9 Final Thruster Fault Isolation - Second Stage

In this section, a method to uniquely isolate a single thruster fault is proposed by evaluating the EKF-based torque bias estimate together with the directional cosine approach. This method represents the second stage of the overall isolation strategy.

As soon as the faulty thruster group $\mathcal{S}_{Tj}$ is identified at the first stage, the faulty thruster can be easily isolated by examining the angle of the vector $\boldsymbol{r}$ given by (4.20) along the fixed force directions $\boldsymbol{b}_{Fk}, \forall k \in \mathcal{S}_{Tj}$. If the kth thruster is faulty, then vectors $\boldsymbol{r} \in \mathbb{R}^3$ and $\boldsymbol{b}_{Fk} \in \mathbb{R}^3$ should be collinear (owing the fault model (2.74)). The degree of collinearity can be computed using the direction cosine approach: $\theta_d^k = \boldsymbol{b}_{Fk} \cdot \boldsymbol{r}/(\|\boldsymbol{b}_{Fk}\|\|\boldsymbol{r}\|)$, where θ_d^k is the angle between the vectors $\boldsymbol{r}$ and $\boldsymbol{b}_{Fk}$. If $\boldsymbol{r}$ and $\boldsymbol{b}_{Fk}$ are collinear, then $\cos(\theta_d^k) = 1$ (i.e., the angle between the two vectors $\theta_d^k = 0$). Thus, the following isolation rule is proposed to isolate the faulty thruster uniquely:

$$\sigma(t) = \underset{k \in \mathcal{S}_{Tj}}{\arg\min} \left(\rho(t) \frac{\boldsymbol{b}_{Fk} \cdot \boldsymbol{r}(t)}{\|\boldsymbol{b}_{Fk}\|\|\boldsymbol{r}(t)\|} \right), \quad t \geq t_g \tag{4.96}$$

In this equation, ρ determines whether an "open-type" or "closed-type" thruster fault has occurred, see Section 2.3 about fault considerations. The notation "$t \geq t_g$" indicates that this rule is applied only when the NUIO–based strategy (first stage) subscribed and confirmed the fault to the subset $\mathcal{S}_{Tj}$.

With respect to ρ, the following two definitions are adopted depending on the identified thruster group $\mathcal{S}_{Tj}$, i.e.,

a) Definition for j=1,...,4

Recalling the geometrical properties in terms of torque directions (see Fig. 4.2), i.e., that thrusters belonging to the same group $\mathcal{S}_{Tk}, \forall k \in \mathcal{S}_G \backslash \{5\}$ generate torques in the same direction, i.e., $\boldsymbol{b}_{Tk} = \boldsymbol{b}_{Th}, \forall k, h \in \mathcal{S}_{Tj}$, where $j \in \mathcal{S}_G \backslash \{5\}$. This property allows to consider the following definition for ρ when $j \in \mathcal{S}_G \backslash \{5\}$, i.e.,

$$\rho^{(1:4)}(t) = \text{sign}\left(\boldsymbol{b}_{Tk} \cdot \hat{\boldsymbol{T}}_{bias}(t)\right), \quad \text{for any } k \in \mathcal{S}_{Tj}, \quad j \neq 5 \tag{4.97}$$

where $\hat{\boldsymbol{T}}_{bias} \in \mathbb{R}^3$ is the estimate of the real torque bias $\boldsymbol{T}_{bias}$ and sign$(\cdot)$ stands for the signum function. This bias is due to the faulty thruster, see (2.74), and should be understood as

follows[3]

$$\boldsymbol{T}_{bias}(t) = -\boldsymbol{B}_T \boldsymbol{\Psi}(t)\tilde{\boldsymbol{u}}(t), \quad \boldsymbol{\Psi}(t) \neq \boldsymbol{0} \tag{4.98}$$

It is obvious that the two fault types, i.e., "open-type" and "closed-type", result in exactly opposite torque bias (shift) relative to the torque direction $\boldsymbol{b}_{Tk}, \forall k \in \mathcal{S}_{Tj}, j \neq 5$.

The bias (4.98) can be estimated using an EKF based on the nominal ($\boldsymbol{J} \triangleq \boldsymbol{J}_0$) attitude dynamics model (4.25), see for instance [246] for realisation details. Note that in (4.97), the direction vector $\boldsymbol{b}_{Tk}$ can be any from $\mathcal{S}_{Tj}$ since they are equal for all $j \in \mathcal{S}_G \backslash \{5\}$, see discussion in Section 4.1.

b) Definition for j=5

Considering the thruster group 5, it is obvious that the previous strategy cannot be used since $\boldsymbol{b}_{Tk}, k \in \mathcal{S}_{T5}$ are not the unique/same-valued direction vectors, see equation (4.3). However, a special property of thrusters belonging to this subset is that they barely produce any torque in the x- and y-axis. This enables to focus only to z-axis and thus, the following definition of ρ when $j = 5$ is proposed:

$$\rho^{(5)}(t) = f_{Wald}(r_{bias}(t_k)), \qquad j = 5 \tag{4.99}$$

where $r_{bias}(t_k) = \hat{T}^z_{bias}(t_k) - \hat{T}^z_{bias}(t_{k-1})$, $\hat{T}^z_{bias}$ is the third component (i.e., the component on the z-axis) of $\hat{\boldsymbol{T}}_{bias}$ and $f_{Wald}(\cdot)$ stands for the sequential Wald test for the variance applied on r_{bias}. This test can result in three possible situations:

$$f_{Wald}(r_{bias}(t_k)) = \begin{cases} 1 & \textbf{if} \text{ decision in favour of "closed-type"} \\ 0 & \textbf{if} \text{ no decision has been adopted} \\ -1 & \textbf{if} \text{ decision in favour of "open-type"} \end{cases} \tag{4.100}$$

For implementation details of the sequential Wald's test, see Appendix B.1.

Improvement of the Strategy

For the thruster group number 5, taking into account (4.3), it is possible to slightly improve the reliability of the isolation algorithm (4.96) by dividing the set $\mathcal{S}_{T5}$ into two smaller subsets defined as follows

$$\mathcal{S}^a_{T5} = \{3, 12\}, \qquad \mathcal{S}^b_{T5} = \{6, 9\} \tag{4.101}$$

Now, the isolation rule (4.96) can be redefined for $j = 5$ as follows

$$\sigma(t) = \begin{cases} \underset{k \in \mathcal{S}^a_{T5}}{\arg\min} \left(\rho^{(5)}(t) \frac{\boldsymbol{b}_{Fk} \cdot \boldsymbol{r}(t)}{\|\boldsymbol{b}_{Fk}\| \|\boldsymbol{r}(t)\|} \right), & \textbf{if} \ \min\limits_{k \in \mathcal{S}^a_{T5}} \rho^{(5)}(t) \left(\boldsymbol{b}_{Tk} \cdot \hat{\boldsymbol{T}}_{bias} \right) \geq \min\limits_{k \in \mathcal{S}^b_{T5}} \rho^{(5)}(t) \left(\boldsymbol{b}_{Tk} \cdot \hat{\boldsymbol{T}}_{bias} \right) \\ \underset{k \in \mathcal{S}^b_{T5}}{\arg\min} \left(\rho^{(5)}(t) \frac{\boldsymbol{b}_{Fk} \cdot \boldsymbol{r}(t)}{\|\boldsymbol{b}_{Fk}\| \|\boldsymbol{r}(t)\|} \right), & \textit{otherwise} \end{cases}$$

Now, the logic (4.96) is able to isolate any of the four considered fault scenarios (see Section 2.3), i.e., thruster fault of both types, within any truster group $\mathcal{S}_{Tj}, \forall j \in \mathcal{S}_G$ (supposing that the

[3] In other words, this bias can be also understood as a difference (bias) between the real torques applied on the spacecraft and the torques as seen from the controller point of view.

thruster group isolation $j = \sigma_g$ was successful).

Since the residual $\boldsymbol{r}$ in (4.96) is matched with the force directions within the already isolated group $\mathcal{S}_{Tj}$, in which the force directions are either exactly opposite ($j \in \mathcal{S}_G \backslash \{5\}$, see (4.2)) or orthogonal ($j = 5$, see (4.3)), this makes the isolation logic $\sigma(t) : \mathbb{R}^+ \times \mathcal{S}_G \to \mathcal{S}_{all}$ very reliable.

Finally, another confirmation window, $\delta > 0$, is introduced according to

$$t_i = \arg\inf_{t \geq t_g + \delta} \{\sigma(t) = \sigma(\vartheta),\ \forall \vartheta \in (t - \delta, t]\} \tag{4.102}$$

where t_i is the isolation time of the faulty thruster. Let $i = \sigma(t_i)$ for future reference.

4.5 Implementation and Tuning of the overall FDI Scheme

Figure 4.5 illustrates the overall structure of the proposed global FDI scheme. It consists of the robust residual generator and the GLR test, both introduced in Section 4.3. The decision test $\varrho^{J_{th}}$ (see (4.22)) triggers the bank of 5 NUIOs and the EKF-based torque bias estimator. Following, the residual signal $\boldsymbol{r}$, torque bias estimate $\hat{\boldsymbol{T}}_{bias}$ and the NUIOs estimation errors are being processed by the two-stage isolation logic introduced in Section 4.4.8 and Section 4.4.9.

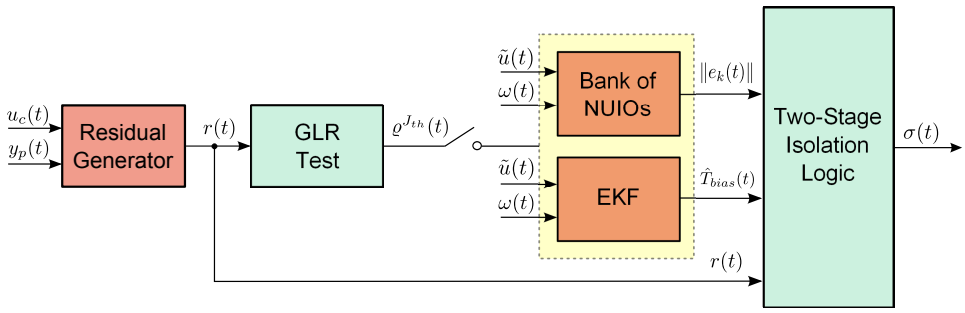


Figure 4.5 – The overall structure of the proposed FDI scheme

The residual generator (4.20) has been designed following the discussion in Section 4.3. The GLR decision test (4.22) has been implemented with $J_{th} = 33$, $T = 0.1$ s, $N_d = 10$ $t_0 = 100$ s and $w_k = 1/3, \forall k \in \{1, 2, 3\}$. The chosen threshold J_{th} has been determined through Monte Carlo simulations to ensure (ideally) a zero false alarm rate. Following the design steps given in Algorithm 2 and the implementation comments in Section 4.4.7, a bank of 5 NUIOs has been designed with the numerical values for α, q, r, β, and κ being fixed to 0, 0.18, 0.05, $\pi/4$, and 0.9 for all NUIOs, respectively. The numerical values of γ and γ^* are found to be 0.9047 and $1.4039e4$.

The well known EKF approach, introduced in Section 1.3.3.1, has been used to estimate the torque bias vector $\boldsymbol{T}_{bias}$. The fourth-order Runge-Kutta integration method has been used to propagate the nonlinear equations [170]. This estimate, i.e., $\hat{\boldsymbol{T}}_{bias}$, is achieved such that the state of the nonlinear (nominal) attitude dynamics is augmented with $\hat{\boldsymbol{T}}_{bias}$, and the so obtained model is used in (1.79). The EKF covariance matrix $\boldsymbol{Q}$ has to be tuned such that the estimated torque bias "directions" are as close as possible to the real ones. This problem can be

mathematically expressed as follows

$$\boldsymbol{Q} = \underset{Q \in \mathbb{R}^{6\times 6}}{\arg\min}\, \text{atan2}\left(\|\boldsymbol{T}_{bias} \times \hat{\boldsymbol{T}}_{bias}(\boldsymbol{Q})\|,\, \boldsymbol{T}_{bias} \cdot \hat{\boldsymbol{T}}_{bias}(\boldsymbol{Q})\right) \tag{4.103}$$

where the atan2(,) function is defined in Appendix A.5.2. It is obvious that, the solution to (4.103), taking into account all the possible fault scenarios and uncertainties, is almost impossible to find. Therefore, the state covariance matrix $\boldsymbol{Q}$ is chosen to be $\boldsymbol{Q} = \text{diag}(\boldsymbol{Q}_\omega, \boldsymbol{Q}_{bias})$, where $\boldsymbol{Q}_\omega = \boldsymbol{I}$ and $\boldsymbol{Q}_{bias} = 0.1\boldsymbol{I}$, and the initial covariance matrix $\boldsymbol{P}_0$ is fixed to $\boldsymbol{P}_0 = \boldsymbol{I}$. The measurement covariance matrix $\boldsymbol{R}$ is selected based on the knowledge of the gyro model, see Section 2.2.1.3 for details.

For the two-stage isolation logic, a confirmation window $\delta_g = 1.5$ s in (4.95) and $\delta = 0.5$ s in (4.102) has been considered, respectively. The whole FDI strategy is summarized in Algorithm 3, see Fig. 4.5 for an illustration.

Algorithm 3 Thruster fault detection and isolation

```
1: if ϱ^{J_th}(t) = 1 then
2:     Decision = declare the fault presence and run the bank of NUIOs;
3:     if σ_g(t) = σ_g(ϑ), ∀ϑ ∈ (t − δ_g, t] then
4:         Decision = declare the thruster group S_{Tj}, j = σ_g(t) to be faulty;
5:         if σ(t) = σ(ϑ), ∀ϑ ∈ (t − δ, t] then
6:             Decision = declare the i^{th} thruster to be faulty, where i = σ(t);
7:         end if
8:     end if
9: end if
```

4.6 Thruster Fault Accommodation

Once a faulty thruster is diagnosed by the aforementioned FDI algorithm, a fault accommodation mechanism has to be engaged in order to maintain the rendezvous/capture objectives of the MSR mission. The nominal 6DOF control law, that is planned to be implemented on-board, is designed to guarantee some predefined performance criteria such as: the chaser attitude misalignment versus the target, the longitudinal and lateral capture velocity errors, the position keeping in the rendezvous corridor, the precise capture accuracy, etc., thus, it is desirable to keep the nominal controller in the loop. For further details, see Chapter 2.

Since the control allocation techniques, introduced in Section 1.4.3, do not require any modifications in the control law (assuming feasibility of the virtual control inputs), it motivates to propose a fault accommodation strategy based on this philosophy. Moreover, the CA solution is further justified by the fact that all the thrusters are individually equipped with a dedicated TLV able to disengage the propellant arrival, switching off *de facto* the associated thruster.

In the next sections, a simple strategy for accommodating the fault effect by changing some functionalities in the TMF function to an online control allocation algorithm is proposed, based on the use of the existing baseline 6DOF controller and TLVs. Figure 4.6 gives an overview of the proposed accommodation solution together with the FDI scheme implemented within the GNC architecture.

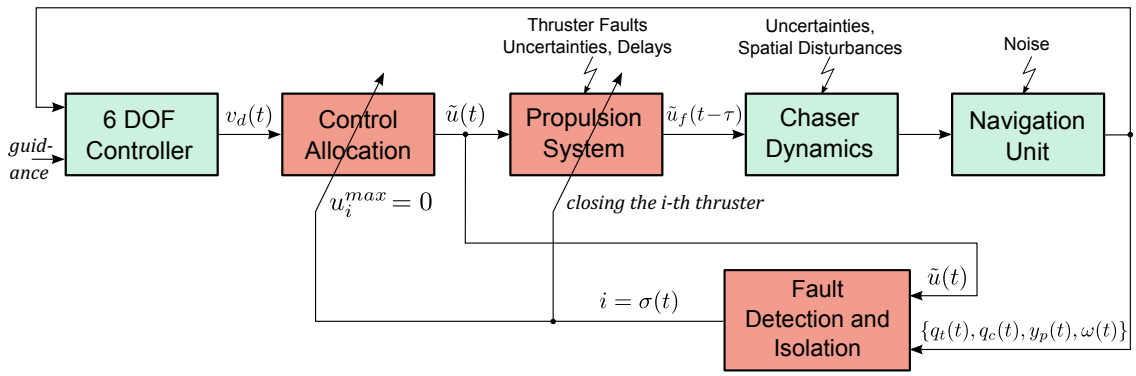


Figure 4.6 – FDI-based fault accommodation strategy implemented within the GNC architecture

4.6.1 Control Re-allocation

During the rendezvous, the chaser control is done on position and attitude and makes use of thrusters only. Thus, a 6DOF control allocation algorithm has to be considered. The on-board CA algorithm shall determine in real-time, i.e., at each control cycle (10 Hz frequency), the proper thruster selection and their firing durations to achieve the controller-commanded torque and force impulses. Hence, the CA algorithm has to perform the following tasks[4]:

- select thrusters capable of performing the controller demand with minimization of the propellant consumption (or another criterion) as far as possible, and
- compute the thruster firing durations while taking into account their firing constraints.

In order to make use of the remaining healthy thrusters in case of an actuator fault, it is required to reconfigure the control allocation scheme (re-allocation) by including the constraints due to the faults. Thus, as soon as the ith thruster is confirmed to be faulty through $\sigma(t)$, see (4.96) and (4.102), the faulty thruster is switched off using the dedicated TLV. The desired forces $\vec{\boldsymbol{F}}_{\tilde{d}}$ and torques $\vec{\boldsymbol{T}}_{\tilde{d}}$ are then re-allocated among the remaining $N-1$ healthy thrusters. This re-allocation can be achieved very easily by changing the constraints in the existing CA algorithm, i.e., if the ith thruster is faulty, then

$$0 \leq \tilde{u}_i \leq 0 \tag{4.104}$$

can counteract the effect of the fault in a simple manner. Additionally, this makes the fault accommodation without any change in the nominal controller or any additional valve position sensor.

Existing CA algorithms which have potential to be used for reconfigurable control allocation (re-allocation) include pseudo-inverse, modified pseudo-inverse, direct allocation, constrained optimization methods based on linear programming or quadratic programming, fixed-point method or their combinations [312]. In the next section, an existing CA approach has been modified and improved in order to cope with the considered FTC problematic.

[4]Note, that what is here called as "Control Allocation (CA) algorithm" is often referred as "Thruster Management Function (TMF)" in the industrial community.

4.6.2 Nonlinear Iterative Pseudoinverse Controller Approach

Here, a modified Nonlinear Iterative Pseudoinverse Controller (NIPC) approach whose original version was proposed by Jin et al. [155], is considered. The NIPC method tries to solve the following optimization problem

$$\begin{aligned} \tilde{\boldsymbol{u}} &= \arg\min_{\tilde{\boldsymbol{u}}} \|\boldsymbol{W}_v \left(\bar{\boldsymbol{B}}\tilde{\boldsymbol{u}} - \boldsymbol{v}_d\right)\|_p \\ \text{s.t. } & 0 \leq \tilde{u}_k \leq \tilde{u}_k^{max},\ \forall k \in \mathcal{S}_{all} \end{aligned} \tag{4.105}$$

where $\bar{\boldsymbol{B}}$ is the overall thruster configuration matrix (see (2.53)), $\boldsymbol{v}_d = [\boldsymbol{T}_{\tilde{d}}^T\ \boldsymbol{F}_{\tilde{d}}^T]^T$ is the vector of the desired torque and force commands of the 6DOF control law[5], and $\tilde{u}_k^{max}$ is the maximum opening duration of the kth thruster. The core of the fault tolerance principle is that if the ith thruster is faulty, then $\tilde{u}_i^{max}$ is set to "0". The weighting matrix $\boldsymbol{W}_v$ affects the prioritization among torque/force components when $\bar{\boldsymbol{B}}\tilde{\boldsymbol{u}} - \boldsymbol{v}_d$ cannot be attained due to thruster constraints.

The different choice of the vector p-norm in (4.105) results in [155]:

1. Minimum flow rate allocation: $\min \|\tilde{\boldsymbol{u}}\|_1$
2. Minimum power allocation: $\min \|\tilde{\boldsymbol{u}}\|_2$
3. Minimum peak torque/force allocation: $\min \|\tilde{\boldsymbol{u}}\|_\infty$

Using the minimum-flow-rate allocation will yield the greatest control authority for flow-rate-limited thruster systems. Similarly for the other two allocations. It is known that stability of the closed-loop system can be guaranteed as long as the constraints of the optimization problem (4.105) are met (feasibility implies stability).

The proposed NIPC method that solves the re-allocation problem to ensure thruster fault tolerance, is given in Algorithm 4. This algorithm also solves the optimization problem (4.105). It terminates if a certain precision $\varepsilon \geq 0$ of the allocated torques/forces, weighted by $\boldsymbol{W}_v$, is achieved (typical choice is $\varepsilon \to 0$) or if the maximum number of iterations N_{iter}^{max} is reached. N_{iter}^{max} can be considered to reflect the max computation burden. In Algorithm 4, MIB (Minimum Impulse Bit)stands for the minimum impulse (minimum shooting time that a thruster can execute), $\lambda > 0$ allows the algorithm to manage the convergence time of the algorithm and $\bar{\boldsymbol{B}}_i^{p+}$ stands for the generalized inverse of $\bar{\boldsymbol{B}}_i$ given in step **3** (optimal in the sense of the considered p-norm).

It is obvious, that both N_{iter}^{max} and λ influence the computational burden of the algorithm. Note, that $\bar{\boldsymbol{B}}_i^{p+}, \forall i \in \mathcal{S}_{all}$ are fixed, thus it is possible to pre-compute them off-line for all $i \in \mathcal{S}_{all}$. This enables also to reduce the computational burden, however the price to pay is a higher memory consumption.

Fault tolerance is achieved due to step **3** and consequently to steps **9** and **12**, the index "i" being determined by the FDI unit. Changing the minimization objective in (4.105) is very simple since it results in changing the criterion $p \in \{1, 2, \infty\}$ in steps **7** and **9**.

Remark 4.7. *It should be noted, that there is no formal proof that the solution of Algorithm 4 will be optimal in the sense of* (4.105)*. Moreover, this algorithm concerns only a finite number of*

[5]Synthesized by the 6DOF controller and followed by the thruster modulator unit, see Section 2.2.3.

Algorithm 4 NIPC control allocation with fault tolerance principle

Set $iter = 0$ and $\boldsymbol{v} = \boldsymbol{v}_d$;
if the ith thruster is declared to be faulty **then**
  Construct $\bar{\boldsymbol{B}}_i$ from $\bar{\boldsymbol{B}}$ such that $\bar{\boldsymbol{b}}_i = \boldsymbol{0}$ and set $\tilde{u}_i^{max} \triangleq 0$;
else
  Set $\bar{\boldsymbol{B}}_i \triangleq \bar{\boldsymbol{B}}$;
end if
while $\|\boldsymbol{W}_v * error\|_p > \varepsilon$ **and** $iter < N_{iter}^{max}$ **do**
  $\boldsymbol{v} = \boldsymbol{v} + \lambda * error$;
  $\tilde{\boldsymbol{u}}^{pc} = \bar{\boldsymbol{B}}_i^{p+} \boldsymbol{v}$;
  $\tilde{\boldsymbol{u}}^{c} = (\tilde{\boldsymbol{u}}^{pc} + |\tilde{\boldsymbol{u}}^{pc}|)/2$;
  for $k = 1$ to N **do**
    if $\tilde{u}_k^c > \tilde{u}_k^{max}$ **then** $\tilde{u}_k^c = \tilde{u}_k^{max}$; **end if**
    if $\tilde{u}_k^c < MIB/2$ **then** $\tilde{u}_k^c = 0$; **end if**
    if $MIB/2 \leq \tilde{u}_k^c < MIB$ **then** $\tilde{u}_k^c = MIB$; **end if**
  end for
  $error = \bar{\boldsymbol{B}}_i \tilde{\boldsymbol{u}}^c - \boldsymbol{v}_d$;
  $iter = iter + 1$;
end while
Set $\tilde{\boldsymbol{u}} \triangleq \tilde{\boldsymbol{u}}^c$;

iterations. Thus, stability proof cannot be provided as stability regards behaviour for iter $\rightarrow +\infty$.

The form in which the NIPC algorithm has been reported here is slightly different with respect to the one in the original reference [155]. Especially because of:

- inclusion of the fault tolerance principle described earlier,
- inclusion of the two stopping rule parameters (i.e., ε and N_{iter}^{max}), and
- taking into account thruster nonlinearities such as MIB.

In the next section, the effectiveness of the NIPC algorithm is evaluated and compared to other approaches.

4.6.3 Comparison of the NIPC Algorithm with the Existing Methods

Figure 4.7 illustrates the performance of 7 CA algorithms introduced in Chapter 1 together with the NIPC algorithm presented earlier. The error signals in blue correspond to $\|\bar{\boldsymbol{B}}\tilde{\boldsymbol{u}}(t) - \boldsymbol{v}_d(t)\|$ over the time interval $t \in [0, 1331.1]$, where $\tilde{\boldsymbol{u}}$ are generated in different ways depending on the considered CA algorithm. These results consider only 11 thrusters for CA purposes. To be more precise, thruster No.1 is considered to be unavailable, thus not taken into account in the CA formulations ($\tilde{u}_1^{max} = 0$). This, in terms of FTC, corresponds to a situation when the FDI unit correctly identified the faulty thruster. The thruster was then immediately closed and the CA was modified accordingly, i.e., a perfect accommodation was achieved.

A sequence of desired force/moment vectors, $\boldsymbol{v}_d(k), k = 0, 1, \ldots$, has been used as the virtual input for these algorithms. This sequence corresponds to a real flight scenario of the rendezvous phase. The desired (virtual) control inputs ($\boldsymbol{v}_d$), synthesized by the 6DOF controller, have been simulated and stored in closed loop, while the results presented in Fig. 4.7 have been performed

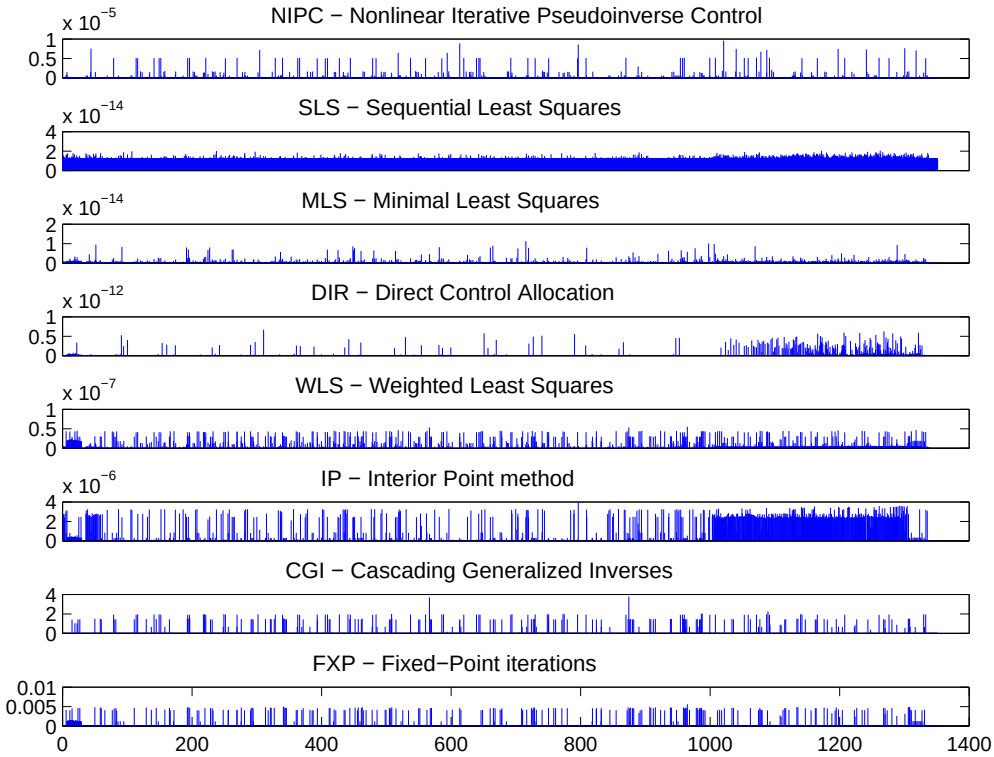


Figure 4.7 – Comparison of the NIPC approach with 7 other CA algorithms taking into account only N-1 thrusters

off-line using the stored sequence (open loop). To better appreciate the pure CA performances, uncertainties on CoM and thruster rise times, as well as constraints such as quantization step and MIB, were not considered in the open loop simulations. On the other hand, all considered CA methods have taken into account the thrusters' saturation limits.

As it can be seen from Fig. 4.7, all the CA methods deliver only approximate solutions of varying accuracy. This, however, to certain amount is not an issue since the final precision highly depends on the considered uncertainties. For instance, the thruster configuration matrix (necessary for all CA algorithms) is not precisely known on-board, therefore even if the CA produces an exact solution, the real torques/forces applied to the spacecraft will differ from the ones supplied to the CA algorithm.

The computational requirements of a particular CA algorithm are a concern if it has to be used on-board. Table 4.1 compares the computational burden of the 8 CA algorithms used to produce Fig. 4.7. The computational load of each algorithm is expressed as a percentage ratio with respect to the SLS algorithm considered to be the reference time (since the SLS algorithm is one of the most computational expensive algorithms).

CA algorithm	NIPC	SLS	MLS	DIR	WLS	IP	CGI	FXP
Computational burden (%)	1.65	100	1.64	31.97	0.85	2.48	0.57	2.01

Table 4.1 – Comparison of the CA algorithms in terms of computational burden

All the simulations have been performed in MATLAB®7.3 running on 2.53GHz Intel® Core™ i5 CPU. The `tic` and `toc` commands were used to compute the timing properties which were

evaluated over the whole length of the simulation. The selected parameters for the NIPC algorithm correspond to: $\boldsymbol{W}_v = \boldsymbol{I}$, $N_{iter}^{max} = 350$, $\lambda = 1.89$, $\varepsilon = 1e-7$ and $p = 2$, i.e., the 2nd norm was chosen leading to a minimum power allocation (see Section 4.6.2 for details about norm selection). The parameters for the other 7 algorithms have been selected to be the same as those of the NIPC algorithm, whenever applicable.

From Fig. 4.7 and Table 4.1 it turns out that the NIPC approach constitutes a good trade-off between accuracy and computational burden. This is mostly because it makes use of the pseudoinverse to make the algorithm conceptually very simple. Another alternative is the WLS algorithm showing very low computational burden and high accuracy.

Remark 4.8. *Note that the MIB constraint was not used in the open loop simulations. Thus, it is expected that the NIPC algorithm might perform even better in real flight scenario (closed loop simulation) when compared with these 7 algorithms. In the next section, the NIPC algorithm is further evaluated/justified in a closed loop manner. However a comparison with the other algorithms is omitted due to very heavy computational complexity of some algorithms, see Table 4.1.*

4.7 Simulation Results

The overall FTC strategy described in the previous sections and illustrated in Fig. 4.5 and Fig. 4.6 has been implemented within the MSR simulator. The NIPC algorithm has been selected and implemented as an integral part of the TMF. All the simulation examples in this section are carried out under realistic conditions (see discussion in Chapter 2) and during the last 20m of the rendezvous phase.

4.7.1 Illustrative Examples

Figure 4.8 serves as the first simulation example and aims to highlight the need for an active FTC solution. This example corresponds to a fully open thruster fault (thruster provides maximum thrust regardless of the control signal) occurring at $t_f = 1100$ s and affecting thruster No.7. To emphasize the relevance of the engagement of the proposed FTC scheme into the GNC system, two identical simulations are carried out. First, when the proposed FTC strategy is active (FTC on), and second, when it is disengaged (FTC off).

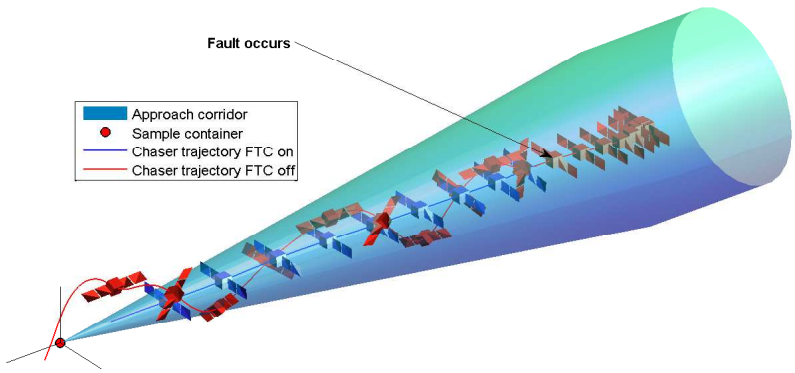


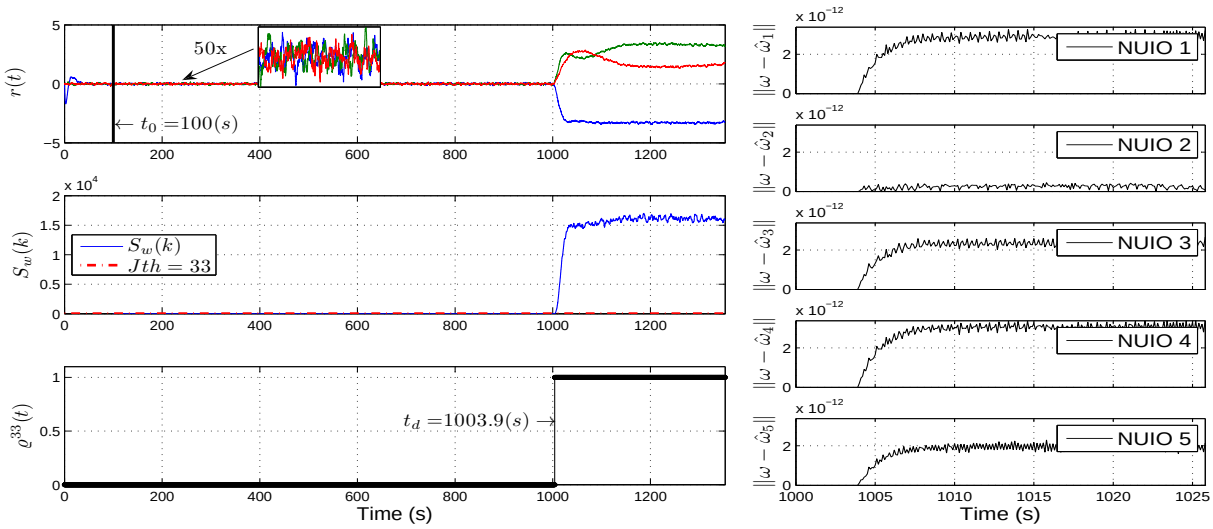
Figure 4.8 – Chaser trajectory within the MSR rendezvous corridor

Figure 4.8 clearly illustrates the consequence when such a fault is not accommodated, i.e., the chaser misses the target and the mission fails. On the other hand, when the proposed approach is engaged, the chaser maintains nominal trajectory, i.e., stays inside the rendezvous corridor and the MSR capture requirements are met. Furthermore, it can be inferred from Fig.4.8 that the chaser keeps its attitude pointing towards the target all the time.

The second and third simulation example aim to illustrate the time behaviour of the internal signals of the proposed FDI scheme in the case of "open-type" and "closed-type" thruster fault. In order to better visually appreciate the obtained FDI signals, the fault accommodation mechanism is switched off for this purpose.

Open-type Thruster Fault Example

Figure 4.9 and Figure 4.10 correspond to a 15% leakage fault affecting the thruster No.2 from $t_f = 1000$ s. The fault is maintained during the whole length of the simulation and is not accommodated (FTC off). The fault presence is declared at $t_d = 1003.9$ s and the faulty thruster index clearly isolates and confirms at $t_i = 1006$ s. It should be noted that the torque bias estimate, shown in Fig. 4.10b, is tuned such that it attains the real torque bias "directions" and is not considered to deliver a trustworthy estimate of the bias magnitude. The same reasoning is valid for Fig. 4.12b.

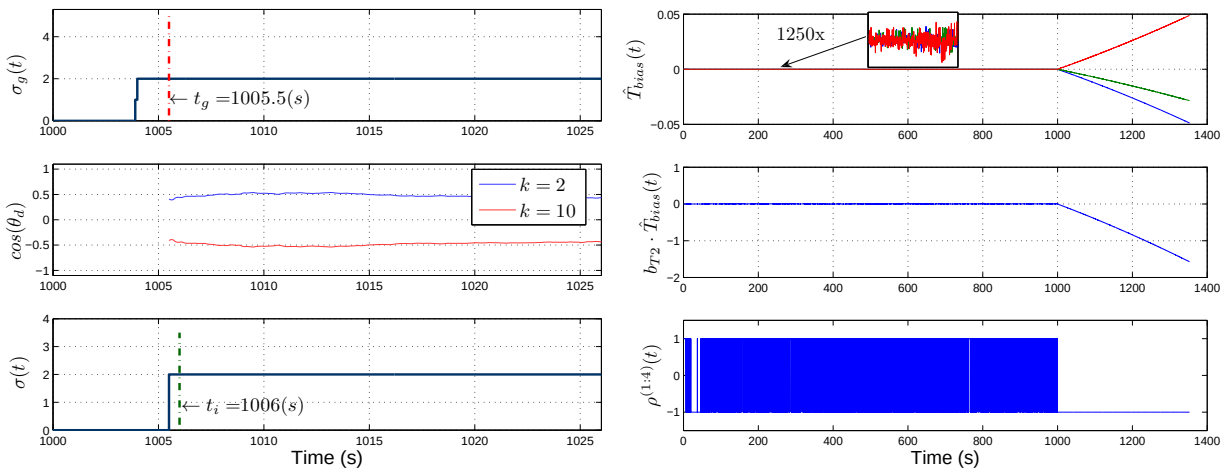


(a) Residual (top), GLR test (middle) and decision test (bottom) (b) Norms of the NUIO estimation errors

Figure 4.9 – Fault detection algorithm and NUIOs' dynamics behaviour for "open-type" fault

Closed-type Thruster Fault Example

Figure 4.11 and Figure 4.12 correspond to a fully blocked thruster failure. The selected faulty thruster is the thruster No.9. This is to illustrate the more complex isolation logic used for the 5th thruster group since $\{9\} \in \mathcal{S}_{T5}$. Again, the fault starts from $t_f = 1000$ s and is maintained. In this case, since this type of fault is much harder to detect and isolate, the fault presence is declared later than in the previous example, i.e., at $t_d = 10018.5$ s. As it can be seen from Fig. 4.12a, there exists a chattering phenomena in the thruster group isolation rule σ_g. Thanks

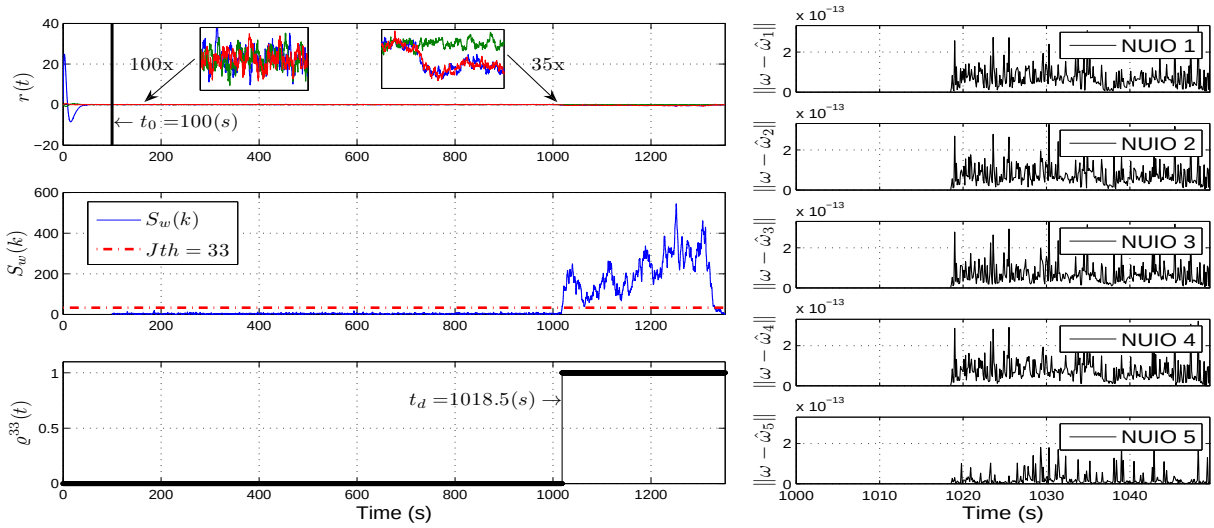


(a) Thruster group isolation (top), directional cosines (middle) and isolation rule signal (bottom)

(b) Torque bias directions estimate (top), bias direction relative to isolated group (middle) and its sign (bottom)

Figure 4.10 – The overall isolation logic behaviour for "open-type" fault

to the judiciously chosen confirmation time ($\delta_g = 1.5$ s), this phenomenon is correctly managed and the correct group is isolated. As it can be further inferred, despite the external disturbances, uncertainties, delays, navigation imperfections, etc., the right thruster index has been isolated at $t_i = 1029.4$s.



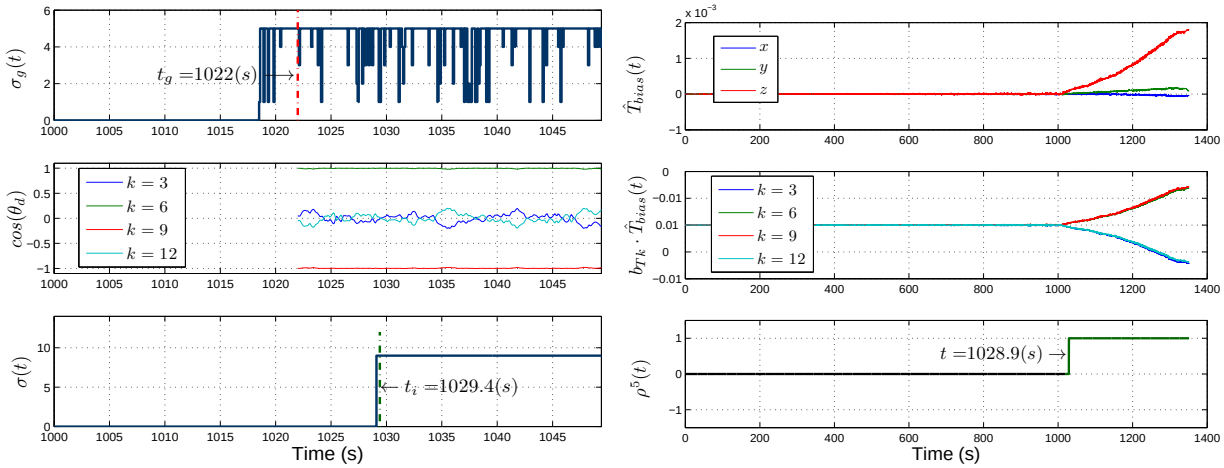
(a) Residual (top), GLR test (middle) and decision test (bottom)

(b) Norms of the NUIO estimation errors

Figure 4.11 – Fault detection algorithm and NUIOs' dynamics behaviour for "closed-type" fault

4.7.2 Monte Carlo Campaign

Several uncertainties are involved in the validation of the FDI/FTC system, from the variation of the initial conditions to the parametric uncertainties in the different components of the chaser spacecraft, see Table 2.3 from Chapter 2 that gives a list of the considered uncertainties. Therefore, a Monte Carlo simulation campaign is used to test and validate the performance of



(a) Faulty thruster group isolation (top), directional cosines within the isolated group (middle) and isolation rule signal (bottom)

(b) Torque bias direction estimates (top), bias directions relative to torque directions within the isolated group (middle) and the Wald's test behaviour (bottom)

Figure 4.12 – The overall isolation logic behaviour for "closed-type" fault

the proposed FDI/FTC system when applied on a number of simulation models with randomly drawn dynamics. In this simulation study, the considered thruster fault scenarios are associated with (see Section 2.3.3 for details on fault modelling):

- **Case 1:** fully open thruster ($m_{leak}(t) = 1, \forall t \geq t_f$);
- **Case 2:** bipropellant leakage ranging from 7% to 20% ($m_{leak}(t) \sim \mathcal{U}(0.07, 0.2), \forall t \geq t_f$);
- **Case 3:** loss of efficiency ranging from 30% to 100% ($\hat{m}_{loss} \sim \mathcal{U}(0.3, 1)$).

The selected leakage and efficiency loss intervals have been determined based on the author's study presented in [91], where it was shown that if the FDI unit fails to detect or isolate a small thruster fault (e.g., $m_{loss} \lesssim 15\%$), the effect that this fault has on the GNC system and/or on the final MSR capture performance requirements is negligible. This is due to the fact that such relatively small fault has a very little impact on the system dynamics and shall be compensated by a robust control law. On the other hand, such faults are very hard or even impossible to detect and isolate.

For each above mentioned fault case, a set of $n_{mc} = 1000$ Monte Carlo simulations has been carried out in order to assess the performance of the proposed FTC strategy. Thruster faults are uniformly distributed among all the 12 thrusters. In all the cases, fault occurs at time $t_f = 1000$ s and is maintained.

All simulations ($3 \times n_{mc}$) have been carried out under realistic conditions, i.e., the navigation unit is considered to deliver "non-perfect" state estimates, therefore all the signals used by the FDI scheme, by the NIPC algorithm and by the 6DOF controller are replaced with their respective uncertain values, see Section 2.2.1 for navigation uncertainty models. Time-varying delays, uncertainties on thruster rise times and spatial disturbances are also considered. For each run, the nominal model parameters, e.g., mass, center of mass, etc., were scattered within a specific limit (see Table 2.3 for details). Since the real configuration matrix $\bar{\boldsymbol{B}}$ is never precisely known on-board, an uncertain configuration matrix $\hat{\boldsymbol{B}}$ is considered for on-board computational purposes (control law, FDI/FTC). Therefore, $\hat{\boldsymbol{B}}$ is considered instead of $\bar{\boldsymbol{B}}$ in the NIPC algorithm.

Metric	Fully open	Leakage	Thrust loss
$\mu(\tau_d)/\sigma(\tau_d)$	2.36/0.14 (s)	4.97/0.75 (s)	48.44/53.29 (s)
$\mu(\tau_g)/\sigma(\tau_g)$	1.50/0.86 (s)	1.75/0.37 (s)	3.37/5.16 (s)
$\mu(\tau_i)/\sigma(\tau_i)$	0.40/0.00 (s)	3.70/11.39 (s)	4.20/8.21 (s)
$\mu(\tau_o)/\sigma(\tau_o)$	4.27/0.87 (s)	10.41/11.71 (s)	56.01/54.57 (s)
p_f	0	0	0.11

Table 4.2 – FDI performances based on 3×1000 Monte Carlo runs

This matrix is computed similarly as $\bar{\boldsymbol{B}}$ in (2.53), but using a worst-case scenario when an offset of -3 cm is added to each axis of the nominal CoM (see Table 2.3).

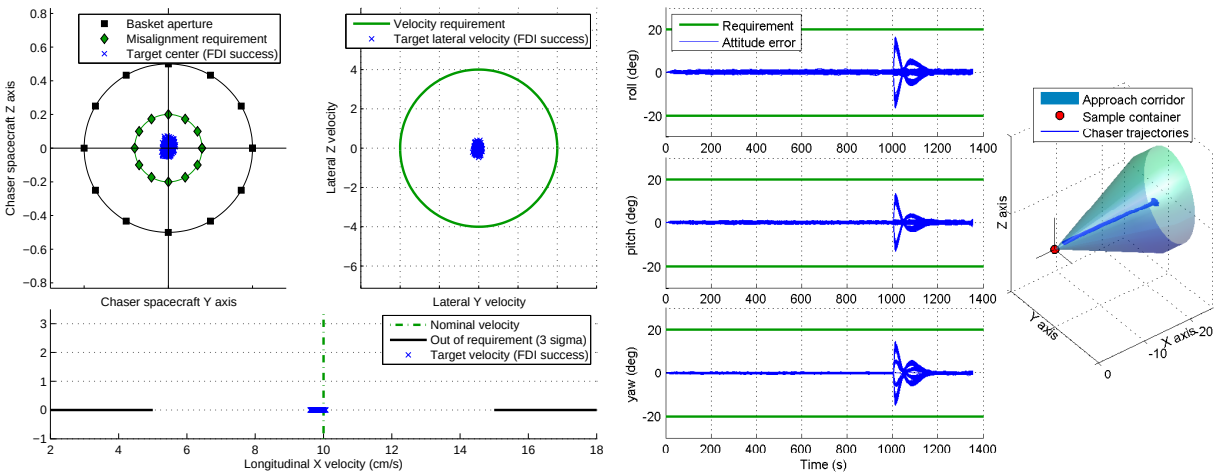
To evaluate the performance and reliability of the proposed FDI scheme, some statistical indices have been used, e.g., the mean detection delay and its corresponding standard deviation. The considered indices are listed below:

- $\mu(\tau_d)/\sigma(\tau_d)$ - mean/standard deviation (st.dev.) of the detection delay (i.e., $\tau_d = t_d - t_f$),
- $\mu(\tau_g)/\sigma(\tau_g)$ - mean/st.dev. of the thruster group isolation delay (i.e., $\tau_g = t_g - t_d$),
- $\mu(\tau_i)/\sigma(\tau_i)$ - mean/st.dev. of the thruster isolation delay (i.e., $\tau_i = t_i - t_g$),
- $\mu(\tau_o)/\sigma(\tau_o)$ - mean/st.dev. of the overall detection and isolation delay (i.e., $\tau_o = t_i - t_f$),
- p_f - FDI fail rate, i.e., the number of wrongly isolated thrusters divided by the total number of Monte Carlo runs (1000 for each fault scenario).

These performance indices have been calculated for each fault case separately. Table 4.2 presents complete results obtained from the simulation campaign. This table demonstrates that the proposed FDI scheme is able to detect and isolate the considered thruster faults within reasonable times. Moreover, it presents a good reliability since no fail detection/isolation has been revealed for the first two faulty scenarios, i.e., $p_f = 0$. Considering the thrust loss scenario, in about 110 simulation cases, the FDI unit failed to either detect or correctly isolate the faulty thruster. As it will be shown in the next, this fact does not violate any capture conditions nor endanger the mission success. Therefore, it can be concluded that the nonlinear simulations clearly demonstrate that all severe faults are detected and isolated by the proposed FDI units within a reasonable time, i.e., such that the required GNC performances are kept (e.g., in terms of pointing accuracy).

Figures 4.14-4.18 illustrate the fault tolerant capabilities of the proposed technique. The capture conditions in terms of position and velocities are given in Fig. 4.13a, Fig. 4.15a, and Fig. 4.17a for fully open thruster, leaking thruster and loss of efficiency thruster fault, respectively. Figure 4.13b, Fig. 4.15b and Fig. 4.17b illustrate, that in all faulty cases, the chaser maintains the required trajectory, i.e., stays inside the rendezvous corridor, and that it keeps its attitude pointing towards the target leading to a successful capture. Finally, Fig. 4.14b, Fig. 4.16b and Fig. 4.18b show that the proposed strategy is able to meet the required 3σ capture accuracy in terms of angular misalignment and angular rate errors.

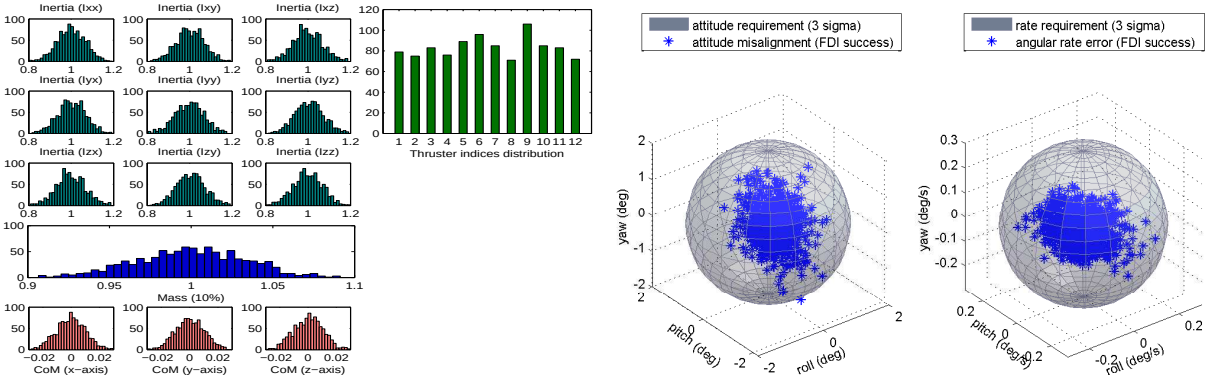
Note, that the early detection of the occurrence of incipient or small size thruster faults (e.g., small thrust loss) is clearly more difficult. Another problem can arise when a fully blocked thruster (i.e., $\hat{m}_{loss} = 1$) is not commanded and thus a fault detection is almost impossible. As



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser attitude error (left) and trajectory inside the rendezvous corridor (right)

Figure 4.13 – Capture position requirements and GNC performances for fault the Case 1



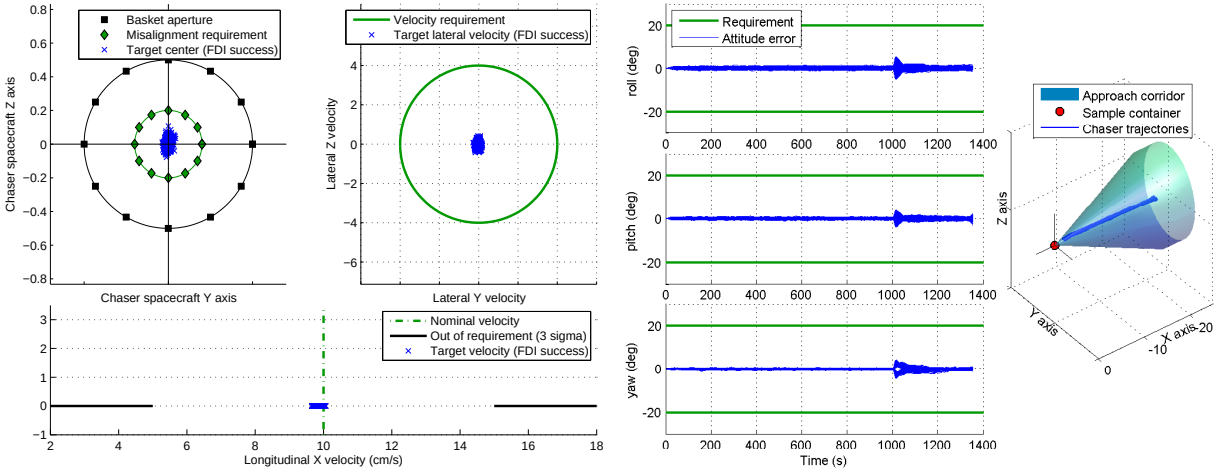
(a) Inertia (top left), mass (middle left), CoM (bottom left) and thruster indices (top right) distribution

(b) Angular misalignment (left) and angular rate error (right) at capture

Figure 4.14 – Considered distributions and capture angular requirements for fault the Case 1

seen in Fig. 4.17a and Fig. 4.17b, despite the fact that in some cases the FDI unit failed, the required capture tolerances and attitude/trajectory conditions are fully met.

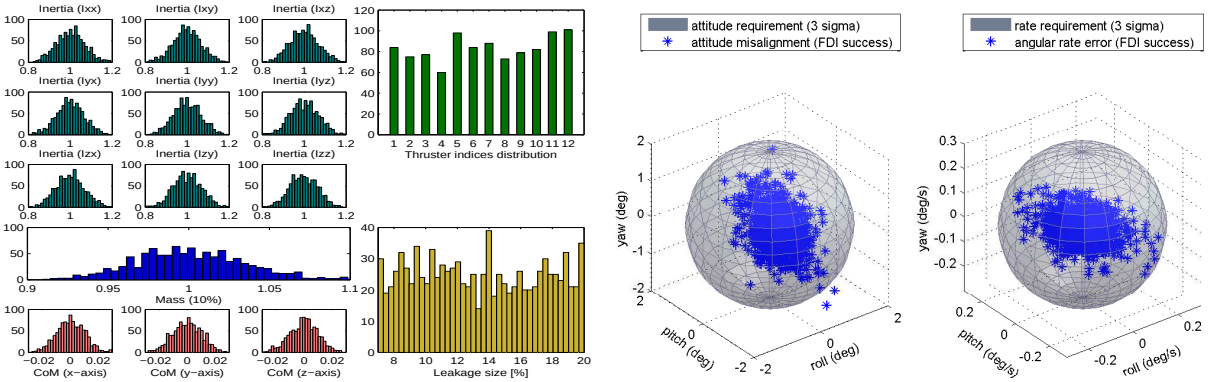
On the other hand, in some particular cases, the attitude misalignment requirement (3-sigma) is not met even if the FDI unit succeeded. This is the case when it takes too long time for the FDI unit to detect and/or isolate the faulty thruster, thus the fault accommodation unit has not enough time to fully recover the faulty system or when the control accuracy has been degraded, e.g., due to a worst case uncertainty or strong disturbance. Based on the FDI performances given in Table 4.2, this case has been very rarely observed. In such cases, the solution may consist in a corrective maneuver that is engaged at the higher level of the fault management unit, see Chapter 2 if necessary.



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser attitude error (left) and trajectory inside the rendezvous corridor (right)

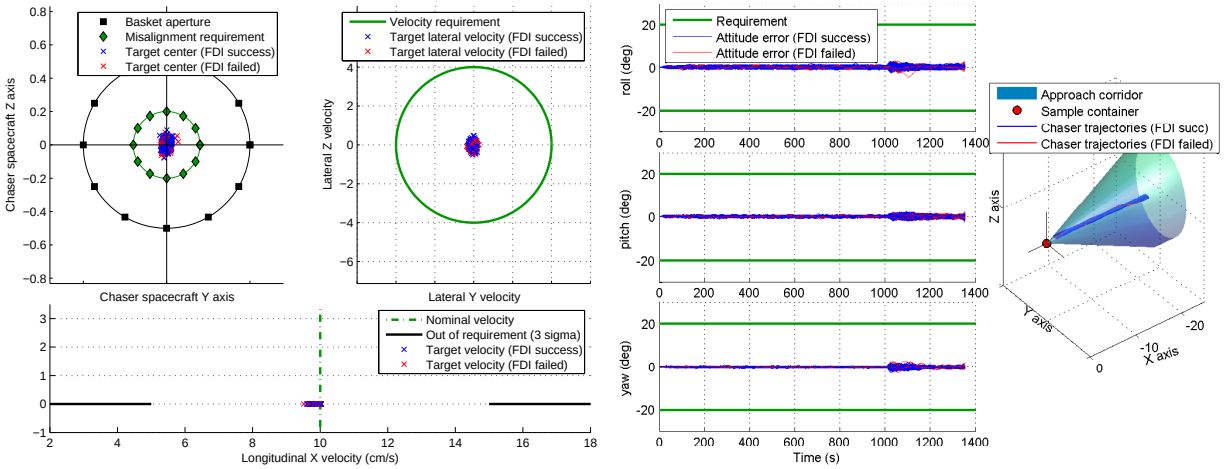
Figure 4.15 – Capture position requirements and GNC performances for fault the Case 2



(a) Inertia (top left), mass (middle left), CoM (bottom left), thruster indices (top right) and leakage size (bottom right) distribution

(b) Angular misalignment (left) and angular rate error (right) at capture

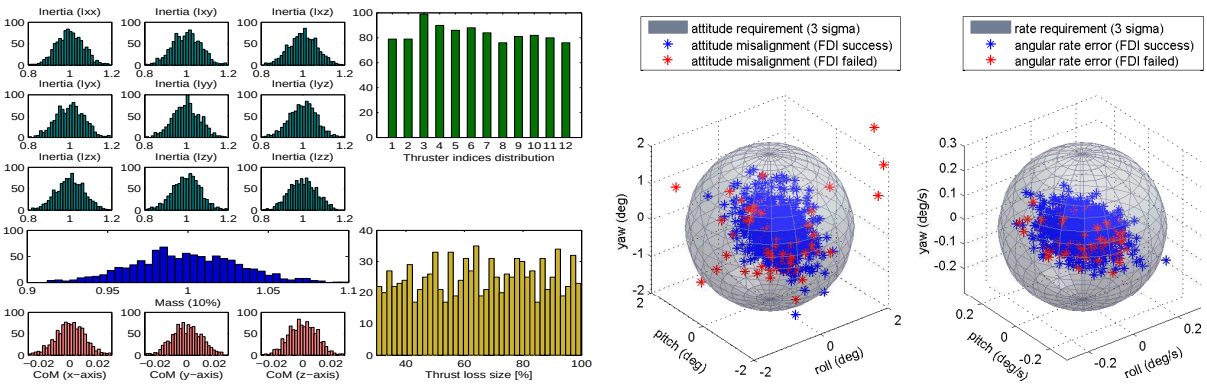
Figure 4.16 – Considered distributions and capture angular requirements for fault the Case 2



(a) Position misalignment on +X face (top left), lateral velocity (top right) and longitudinal velocity (bottom)

(b) Chaser attitude error (left) and trajectory inside the rendezvous corridor (right)

Figure 4.17 – Capture position requirements and GNC performances for fault the Case 3



(a) Inertia (top left), mass (middle left), CoM (bottom left), thruster indices (top right) and thrust loss size (bottom right) distribution

(b) Angular misalignment (left) and angular rate error (right) at capture

Figure 4.18 – Considered distributions and capture angular requirements for fault the Case 3

4.8 Conclusion

In this chapter, a systematic procedure has been presented for the theoretical design and application of a model-based approach to FDI/FTC of an autonomous rendezvous system in the terminal phase. The aim is to detect and isolate a single thruster fault affecting the chaser propulsion system and to accommodate it as quick as possible. The proposed FDI scheme is based on a robust fault detector and a NUIO-based isolation logic. The NUIO gains are given by an LMI optimization, which ensures maximization of the admissible Lipschitz constant while simultaneously satisfying the $\mathcal{L}_2$ gain bound and the pole constraints on the observer dynamics. The $\mathcal{L}_2$ attenuation is considered to minimize the effect of the uncertain inertia on the state estimation error. The NUIO design together with the derivation of the uncertain inertia inverse can be considered as a contribution to the theory. The thruster fault tolerance is achieved by an improved version of the NIPC control allocation algorithm scheduled by the robust FDI scheme. A Monte Carlo simulation campaign has been performed to assess the performance and robustness of the NUIO-based FDI/FTC system subject to parameter uncertainties, spatial disturbances, delays and imperfect navigation. The results indicate that, for all considered fault profiles, which are those considered to be the most relevant by the industrial partners, the proposed strategy can carry out the terminal rendezvous successfully and meet all the required capture specifications.

Conclusions and Perspective

"You cannot create experience. You must undergo it."
— Albert Camus, French Nobel Prize winner

This thesis dealt with the design and validation of advanced model-based methodologies for an integration of FTC capabilities within the GNC system of a chaser spacecraft to ensure a success rendezvous with a target in a circular orbit around the planet of Mars. The main objective, conclusive work of a three years research period focused on the major of fault diagnosis and fault-tolerant control, was to present a collection of results which should lead towards a unified framework for FTC of an autonomous spacecraft involved in a safety critical mission, like MSR mission, PROBA 3, etc.. The analysis is conducted in the context of a terminal rendezvous sequence for the Mars Sample Return mission.,

In space systems, fault tolerance is usually achieved by Fault/Failure Detection Isolation and Recovery approach. FDIR solutions are preferred to FTC ones due to their availability and simplicity. In the FDIR problem, when a fault is diagnosed and subscribed to a subsystem, the redundant subsystem is activated in order to recover the initial performance. That is what the "R" means in the acronym FDIR. The FTC solutions differ fundamentally from the FDIR ones, since they are not based on a redundant system/subsystems (e.g., actuators and sensors), but they are rather based on analytical (software) redundancy (e.g., model-based approaches for fault detection and isolation and/or functional redundancy in actuators for fault tolerance). Due to the increasing mission demands and the strict constraints on weight, power and cost, providing full hardware redundancy for all actuators is difficult. In order to overcome these limitations, this thesis investigated some methodologies required to design and incorporate an FTC system that performs its functions autonomously and it is based on analytical redundancy, where applicable.

The review of the available state of the art on existing FTC system concepts and FDI approaches, and their possibility to be applied for space systems, has concluded that there exist some important learned lessons:

i) The first is that the tolerance to both sensor and actuator faults cannot be achieved at the same level. The reason is quite evident: since any model-based FDI/FTC scheme uses the sensor measurements $\boldsymbol{y}$, one has to be sure that these measurements are fault-free. Similarly for tolerance to sensor faults, because FTC scheme like observer-based method

uses the control signals $\boldsymbol{u}$, one has to be sure that no faults occur in the actuators. As a direct consequence, for space systems, it is better to hierarchize the fault diagnosis task into different levels and to use hardware redundancy in sensors or signal-based techniques in order to guarantee sensor fault tolerance. A direct consequence of this is that a global FTC system should ensure tolerance to sensor faults first, and then if the measurements are deemed to be "fail-safe", the second step should consist in ensuring tolerance to actuator faults that is at an upper level than sensor fault tolerance. Here, advanced model-based techniques for FDI and control allocation are proposed for fault accommodation.

ii) Another lesson is that the FTC requirements should not be decoupled from mission objectives. If the already in-placed robust GNC system is able to compensate some subset of thruster faults (e.g., small losses of thruster efficiency), then there is no need to develop a FTC system for this subset (see Fig. 4.17 and Fig. 4.18b in Chapter 4 or Fonod et al. [91] if necessary).

iii) Finally, because of the lack of formal proofs, both in terms of global stability and performance, for many methods (see Table 1.2 and Table 1.1 in Chapter 1), the control reallocation approach for FTC purpose seems to be the more advantageous one in the case of functional redundancy based thruster configuration, since it requires a little modification of the existing GNC system.

The solutions investigated in this thesis followed these kinds of strategies.

This work has conducted a survey chapter which illustrated some concepts, definitions and classical results as well as some examples from successful implementation of FDI and FTC approaches in some space missions. Then, a complete description of the already in-placed GNC system and of the failure management unit has been addressed. Within the studies conducted in this thesis, two different thruster configurations have been studied. The first (baseline) configuration disposes with a fully redundant thruster set of 2x8 thrusters, whilst the second configuration is composed of 12 thrusters with functional redundancy. Starting from these concepts, two architectures for FDIR and FTC have been considered. These architectures have been developed in order to accomplish the task of fault tolerance in the more efficient way.

For the baseline configuration, two distinct model-based FDIR schemes for thruster fault diagnosis and accommodation have been proposed. The first scheme is based on the position model whereas the second scheme is based on the attitude model. Effects of unknown time-varying delays induced by the propulsion drive electronics and uncertainties on the thruster rise times have been taken into account during the robust FDI scheme design procedure. The proposed FDI strategy is based exclusively on one observer and uses a cross-correlation like isolation test computed on a sliding window. Therefore, the computational burdens is kept low, which is an a priori condition for real time on-board implementation. The proposed recovery action consists in disengaging the faulty thruster using a dedicated thruster latch valve and redirecting the control signal to the back-up thruster in the redundant thruster set. This solution to fault accommodation does not require any change in the nominal controller or TMF, which leads the solution being very attractive from an industrial perspective. For the validation purposes, four different real fault scenarios were investigated. The obtained results from a Monte Carlo simulation campaign, performed under realistic conditions considering imperfect navigation unit, delays, spatial disturbances (gravity gradient, atmospheric drag, and solar radiation pressure) and parameter uncertainties (mass, inertia, center of mass, and uncertainties on the thruster rise times), revealed that the proposed FDI strategies are effective. They also showed that all

the considered fault scenarios are covered with the suggested model-based FDI schemes, i.e., they are able to unambiguously isolate all considered faults with high probability. Moreover, the carefully selected FDI performance indices also reveal that the position model-based scheme tends to achieve very similar performance as the scheme based on the pure attitude model. The position model-based scheme succeeded thanks to the judiciously chosen linear model, i.e., a model that takes into account both the rotational and translational motions of the chaser. In this model, the attitude quaternion plays the role of a scheduling parameter for the residual generation.

An active FTC system strategy to detect, isolate and accommodate a thruster fault has been proposed for the second thruster configuration. A robust fault detector, based on a residual generator with enhanced robustness against the uncertain input delay, has been suggested for fault detection purposes. For fault isolation, a bank of robust NUIOs has been proposed. Based on a set of explicit rules, an isolation strategy has been given to unambiguously isolate a single thruster fault affecting the chaser propulsion system. The main challenge of the isolation problem inhered in the fact that the considered thruster configuration consists of a subset of thrusters which produce torque in almost the same directions. The thruster fault tolerance was achieved by an improved version of the NIPC control allocation algorithm scheduled by the robust NUIO-based FDI scheme. A Monte Carlo simulation campaign has been performed to assess the performance and robustness of the proposed FDI/FTC system subject to parameter uncertainties, spatial disturbances, delays and unperfect navigation. The results indicate that, for all considered fault profiles, the proposed strategy can carry out the terminal rendezvous successfully and the required capture accuracy is maintained. Moreover, it was shown that in case of small thruster faults, the required GNC performances are kept (e.g., in terms of pointing accuracy) despite wrong isolation or non-detection. On the other hand, all the severe faults have been detected and isolated by the proposed FDI unit within a reasonable time.

To conclude, all the results obtained in this thesis revealed that both advanced FDIR and FTC techniques have great advantages in terms of reliability, safety and mission success when compared to the classical FDIR approaches. Thanks to the good knowledge of the subsystems that the engineers at ESA and TAS have, the FMEA (Fault Mode and Effect Analysis) made it easier to develop a more specific FDI/FTC schemes dedicated to certain subset of occurring faults in a real spacecraft. This is one of the many reasons why the valuable knowledge of the control system engineers collaborating within this project was crucial.

Future developments should include the study of more complex verification and validation tools that could enlighten more the distributed and uncertain nature of the complex spacecraft systems (variation of the center of mass, more realistic model of the navigation unit, etc.) and also the stochastic nature of the faults. Robustness against other model parameters like flexible modes, slosh phenomena, uncertain mass, variation of the center of mass, etc. should be incorporated at the design stage of the FDI scheme. Moreover, robustness and sensitivity constraints should be considered too, for instance using H_∞/H_- filtering theory. The implementation, performance, reliability and certification issues slow down the use of these techniques in space, therefore the complexity and computational burden should be further reduced or at least kept at the current level.

List of Main Contributions

In the following, a list of contributions in point fashion is presented. At the end of each list entry, a reference number is given which corresponds to the reference number of the author's list of publication given earlier (see page xxiii).

The contributions of this thesis are mainly concerned by:

- the development of two distinct approaches for the FDI of any kind of thruster faults ("open-type" and "closed-type") [1],[2],
- the comparison study of the position model-based FDI scheme with the pure attitude model-based scheme [2],
- the analysis of the impact of small thruster faults on the GNC performance and capture accuracy [4],
- the development of a method for estimating the complex distribution matrix $\boldsymbol{E}_d$ (used to decouple the effect of uncertain input delays from the residual signal) using:
  - LPV transformation based on the first-order Padé approximation [6],
  - polytopic transformation based on the CH (Cayley-Hamilton) theorem [5],[6],[7],
  - combination of two polytopic transformations, one based on the CH theorem and the other based on the h-th order Taylor series expansion [2].
- the derivation of the uncertain inertia matrix inverse decomposed form $\boldsymbol{J}^{-1} = \boldsymbol{J}_0^{-1} + \boldsymbol{R}_2\boldsymbol{\Delta}_2\boldsymbol{S}_2$ [1],
- the development of a NUIO with constrained observer dynamics, bounded $\mathcal{L}_2$ gain from $\Delta\boldsymbol{B}\tilde{\boldsymbol{u}}$ to the estimation error $\boldsymbol{e}$ and maximization of the admissible Lipschitz constant γ^* [1], [3], [4],
- the improvement of the NIPC control allocation algorithm for FTC purposes [1].

Appendix A

Mathematical Details

The purpose of this appendix is to introduce some mathematical results that are used throughout this thesis.

A.1 Lemmas

A.1.1 Neumann Series

Lemma A1 (Neumann Series, [37])**.** *Consider a square matrix $\boldsymbol{A}$ such that $\|\boldsymbol{A}\| < 1$. Let λ be any eigenvalue of $\boldsymbol{A}$. It is clear that $(\boldsymbol{I} - \boldsymbol{A})$ is invertible if $\lambda \neq 1, \forall\lambda \in \Lambda(\boldsymbol{A})$. The condition $\|\boldsymbol{A}\| < 1$ implies that $|\lambda| < 1, \forall\lambda \in \Lambda(\boldsymbol{A})$. Thus, $(\boldsymbol{I} - \boldsymbol{A})$ is invertible and the Neumann series*

$$(\boldsymbol{I} - \boldsymbol{A})^{-1} = \sum_{k=0}^{\infty} \boldsymbol{A}^k = \boldsymbol{I} + \boldsymbol{A} + \boldsymbol{A}^2 + \dots$$

converges. When $\|\boldsymbol{A}\| \geq 1$, $(\boldsymbol{I} - \boldsymbol{A})$ is still invertible if $\lambda \neq 1, \forall\lambda \in \Lambda(\boldsymbol{A})$, but the Neumann series does not converge because $\lim_{k\to\infty} \boldsymbol{A}^k \neq \boldsymbol{0}$.

Proof. Since $\|\boldsymbol{A}\| < 1$, the series $\sum_{k=0}^{\infty} \|\boldsymbol{A}\|^k$ converges. Since $\|\boldsymbol{A}^h\| \leq \|\boldsymbol{A}\|^h$, the series $\sum_{k=0}^{\infty} \boldsymbol{A}^k$ converges, too. Denote by $\boldsymbol{Z}$ its limit. $\boldsymbol{Z}\boldsymbol{A} = \boldsymbol{A}\boldsymbol{Z} = \sum_{k=0}^{\infty} \boldsymbol{A}^{k+1}$; therefore $(\boldsymbol{I} - \boldsymbol{A})\boldsymbol{Z} = \boldsymbol{Z}(\boldsymbol{I} - \boldsymbol{A}) = \boldsymbol{I}$, which proves Lemma A1. ■

A.1.2 Millers's Lemma on the Inverse of the Sum of Matrices

Lemma A2 (Inverse of the Sum of Matrices, Miller [196])**.** *Let $\boldsymbol{A}$ and $(\boldsymbol{A} + \boldsymbol{B})$ be nonsingular matrices and let $\boldsymbol{B}$ have positive rank r. Let $\boldsymbol{B} = \boldsymbol{E}_1 + \boldsymbol{E}_2 + \ldots + \boldsymbol{E}_r$ where each $\boldsymbol{E}_k$ has rank one and $\boldsymbol{C}_{k+1} = \boldsymbol{A} + \boldsymbol{E}_1 + \boldsymbol{E}_2 + \ldots + \boldsymbol{E}_r$ is nonsingular for $k = 1, \ldots, r$. Then if $\boldsymbol{C}_1 = \boldsymbol{A}$,*

$$(\boldsymbol{A} + \boldsymbol{B})^{-1} = \boldsymbol{C}_r^{-1} - g_r \boldsymbol{C}_r^{-1} \boldsymbol{E}_r \boldsymbol{C}_r^{-1}$$

with

$$\boldsymbol{C}_{k+1}^{-1} = \boldsymbol{C}_k^{-1} - g_k \boldsymbol{C}_k^{-1} \boldsymbol{E}_k \boldsymbol{C}_k^{-1}, \quad k = 1, \ldots, r$$

$$g_k = \frac{1}{1 + tr(\boldsymbol{C}_k^{-1}\boldsymbol{E}_k)}$$

where $tr(\cdot)$ stands for the sum of the elements on the main diagonal.

Proof. The proof can be found in Miller [196]. ■

A.1.3 Schur's Complement

Lemma A3 (Schur's Complement)**.** *Consider a matrix $\boldsymbol{X} \in \mathbb{R}^{n\times n}$ partitioned as*

$$\boldsymbol{X} = \begin{bmatrix} \boldsymbol{Q} & \boldsymbol{S} \\ \boldsymbol{S}^T & \boldsymbol{R} \end{bmatrix} > 0$$

where $\boldsymbol{Q} \in \mathbb{R}^{p\times p}$ and $\boldsymbol{Q} \in \mathbb{R}^{q\times q}$, with $n = p + q$. If $\boldsymbol{R}$ is nonsingular, the Schur complement of $\boldsymbol{X}$ with respect to $\boldsymbol{R}$ is defined as

$$\boldsymbol{X}/\boldsymbol{Q} \triangleq \boldsymbol{Q} - \boldsymbol{S}\boldsymbol{R}^{-1}\boldsymbol{S}^T$$

$$\boldsymbol{Q} - \boldsymbol{S}\boldsymbol{R}^{-1}\boldsymbol{S}^T > 0, \quad \boldsymbol{R} > 0$$

Proof. The proof of Schur's complement lemma can be found in [111]. ■

A.1.4 Matrix Inequality Lemma

Lemma A4 (Zhou and Khargonekar [317])**.** *Let $\boldsymbol{D}$, $\boldsymbol{F}$, and $\boldsymbol{\Sigma}(t)$ be matrices with appropriate dimensions. If $\boldsymbol{\Sigma}^T(t)\boldsymbol{\Sigma}(t) \leq \boldsymbol{I}, \forall t$, then for any scalar $\epsilon > 0$ the following inequality holds:*

$$\boldsymbol{D}\boldsymbol{\Sigma}(t)\boldsymbol{F} + \boldsymbol{F}^T\boldsymbol{\Sigma}^T(t)\boldsymbol{D}^T \leq \frac{1}{\epsilon}\boldsymbol{D}\boldsymbol{D}^T + \epsilon\boldsymbol{F}^T\boldsymbol{F}$$

Proof. It can be verified that the following yields

$$\left(\epsilon^{\frac{1}{2}}\boldsymbol{D}^T - \epsilon^{\frac{1}{2}}\boldsymbol{\Sigma}(t)\boldsymbol{F}\right)^T \left(\epsilon^{\frac{1}{2}}\boldsymbol{D}^T - \epsilon^{\frac{1}{2}}\boldsymbol{\Sigma}(t)\boldsymbol{F}\right) \geq 0$$

then expanding the above yields

$$\epsilon^{-1}\boldsymbol{F}^T\boldsymbol{\Sigma}^T(t)\boldsymbol{\Sigma}(t)\boldsymbol{F} + \epsilon\boldsymbol{D}\boldsymbol{D}^T \geq \boldsymbol{D}\boldsymbol{\Sigma}(t)\boldsymbol{F} + \boldsymbol{F}^T\boldsymbol{\Sigma}^T(t)\boldsymbol{D}^T$$

It is obvious that $\|\boldsymbol{\Sigma}\| \leq 1 \Leftrightarrow \lambda_{max}(\boldsymbol{\Sigma}^T\boldsymbol{\Sigma}) \leq 1 \Leftrightarrow \boldsymbol{\Sigma}^T\boldsymbol{\Sigma} \leq \boldsymbol{I}$, thus

$$\epsilon\boldsymbol{D}\boldsymbol{D}^T + \frac{1}{\epsilon}\boldsymbol{E}^T\boldsymbol{E} \geq \epsilon^{-1}\boldsymbol{F}^T\boldsymbol{\Sigma}^T(t)\boldsymbol{\Sigma}(t)\boldsymbol{F} + \epsilon\boldsymbol{D}\boldsymbol{D}^T \geq \boldsymbol{D}\boldsymbol{\Sigma}(t)\boldsymbol{F} + \boldsymbol{F}^T\boldsymbol{\Sigma}^T(t)\boldsymbol{D}^T$$

This concludes the proof. ■

A.2 Norms and Singular Values

A.2.1 Vector Norms

Let $\boldsymbol{u} \in \mathbb{R}^r$, the p-norm $\|\boldsymbol{u}\|_p$ of the vector $\boldsymbol{u}$ is defined as follows

$$\|\boldsymbol{u}\|_p = \left(\sum_{i=1}^{r} |u_i|^p\right)^{1/p}, \qquad 1 \leq p \leq \infty$$

For $p = \{1, 2, \infty\}$ the following vector norms are obtained

$$\|\boldsymbol{u}\|_1 = \sum_{i=1}^{r} |u_i|$$

$$\|\boldsymbol{u}\|_2 = \sqrt{\sum_{i=1}^{r} u_i^2} = \sqrt{\boldsymbol{u}^T\boldsymbol{u}}$$

$$\|\boldsymbol{u}\|_\infty = \lim_{p\to\infty} \left(\sum_{i=1}^{r} |u_i|^p\right)^{1/p} = \max_{1\leq i\leq r} |u_i|$$

The 2-norm $\|\boldsymbol{u}\|_2$ defined above is also called the Euclidian or spectral norm and is used without subscript, i.e., $\|\boldsymbol{u}\|$.

A.2.2 Matrix Norms

Let $\boldsymbol{A} \in \mathbb{R}^{n\times r}$, the matrix p-norm $\|\boldsymbol{A}\|_p$ of the matrix $\boldsymbol{A}$ is defined as

$$\|\boldsymbol{A}\|_p = \sup_{u\neq 0} \frac{\|\boldsymbol{A}\boldsymbol{u}\|_p}{\|\boldsymbol{u}\|_p}, \quad \forall \boldsymbol{u} \in \mathbb{R}^r$$

where sup stands for *supremum* (least upper bound). The norm of a matrix $\boldsymbol{A}$ is defined through the norm of a vector $\boldsymbol{u}$, thus it is called an induced norm. For $p = \{1, 2, \infty\}$ the following matrix norms are obtained

$$\|\boldsymbol{A}\|_1 = \max_{1\leq j\leq r} \sum_{i=1}^{n} |a_{ij}|$$

$$\|\boldsymbol{A}\|_2 = \sqrt{\lambda_{max}(\boldsymbol{A}^T\boldsymbol{A})} = \sigma_{max}(\boldsymbol{A})$$

$$\|\boldsymbol{A}\|_\infty = \max_{1\leq i\leq n} \sum_{j=1}^{r} |a_{ij}|$$

where λ_{max} and σ_{max} denote the largest eigenvalue and singular value of the matrix $\boldsymbol{A}$, respectively.

The Frobenius norm $\|\boldsymbol{A}\|_F$ of the matrix $\boldsymbol{A}$ is defined as

$$\|\boldsymbol{A}\|_F = \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{r} |a_{ij}|^2} = \sqrt{\mathrm{tr}(\boldsymbol{A}^H\boldsymbol{A})}$$

where $\boldsymbol{A}^H$ is the conjugate transpose of $\boldsymbol{A}$.

A.2.3 Signal Norms

Definition A1 ($\mathcal{L}_p$ Space)**.** The space $\mathcal{L}_p$ consists of all $\mathcal{L}$ebensque measurable functions $\boldsymbol{u}(t) : \mathbb{R}^+ \to \mathbb{R}^r$ having a finite $\mathcal{L}_p$ norm $\|\boldsymbol{u}\|_{lp}$.

Let $\boldsymbol{u}(t) : \mathbb{R}^+ \to \mathbb{R}^r$ be a $\mathcal{L}$ebensque measurable function, then the $\mathcal{L}_p$-norm $\|\boldsymbol{u}\|_{lp}$ of the signal $\boldsymbol{u}(t)$ is defined as

$$\|\boldsymbol{u}\|_{lp} = \left(\int_0^\infty \|\boldsymbol{u}(t)\|_p^p dt\right)^{\frac{1}{p}}$$

For $p = \{1, 2, \infty\}$ the following signal norms are obtained

$$\mathcal{L}_1 : \qquad \|\boldsymbol{u}\|_{l1} = \int_0^\infty \|\boldsymbol{u}(t)\|_1 dt$$

$$\mathcal{L}_2 : \qquad \|\boldsymbol{u}\|_{l2} = \sqrt{\int_0^\infty \|\boldsymbol{u}(t)\|^2 dt}$$

$$\mathcal{L}_\infty : \qquad \|\boldsymbol{u}\|_{l\infty} = \sup_{t \geq 0} \|\boldsymbol{u}(t)\|_\infty$$

A.2.4 Singular Values

The *singular values* of $\boldsymbol{A}$ are given by the positive square roots of the eigenvalues of $\boldsymbol{A}^T\boldsymbol{A}$, i.e.,

$$\sigma_i(\boldsymbol{A}) = \sqrt{\lambda_i(\boldsymbol{A}^T\boldsymbol{A})}, \quad i = 1, \ldots, r$$

ordered such that $\sigma_1 \geq ... \geq \sigma_l > \sigma_{l+1} = ... = \sigma_r = 0$, where $l = \text{rank}(\boldsymbol{A})$.

A.3 Pseudoinverses

Let $\boldsymbol{B} \in \mathbb{R}^{l \times r}$, where $r \geq l$ and $l = \text{rank}(\boldsymbol{B})$. Consider solving

$$\boldsymbol{B}\boldsymbol{u} = \boldsymbol{v}$$

for $\boldsymbol{u} \in \mathbb{R}^r$, with given $\boldsymbol{v} \in \mathbb{R}^l$. If $l < r$, there is no unique solution. Any *generalized inverse* $\boldsymbol{G}$ of $\boldsymbol{B}$, satisfying $\boldsymbol{B}\boldsymbol{G} = \boldsymbol{I}$, i.e., any right inverse of $\boldsymbol{B}$, gives the solution

$$\boldsymbol{u} = \boldsymbol{G}\boldsymbol{v}$$

To make the choice of $\boldsymbol{u}$ unique, a minimum norm of the solution can be used, i.e., $\min_u \|\boldsymbol{u}\|_p$, where p is chosen e.g., as $p = \{1, 2, \infty\}$.

A.3.1 Moore-Penrose Pseudoinverse

Lemma A5 (The Moore-Penrose pseudoinverse)**.** *The problem*

$$\min_u \|\boldsymbol{u}\|_2$$

$$\textit{subject to } \boldsymbol{B}\boldsymbol{u} = \boldsymbol{v}$$

where $l = \text{rank}(\boldsymbol{B})$ *and* $r \geq l$*, has the unique solution*

$$\boldsymbol{u} = \boldsymbol{B}^{\dagger}\boldsymbol{v}$$

where

$$\boldsymbol{B}^{\dagger} = \boldsymbol{B}^T(\boldsymbol{B}\boldsymbol{B}^T)^{-1}$$

is the pseudoinverse, or the Moore-Penrose inverse of $\boldsymbol{B}$*.*

Proof. Define the Lagrangian of this problem as

$$L(\boldsymbol{u}, \boldsymbol{\lambda}) = \frac{1}{2}\boldsymbol{u}^T\boldsymbol{u} + \boldsymbol{\lambda}^T(\boldsymbol{v} - \boldsymbol{B}\boldsymbol{u})$$

where $\boldsymbol{\lambda}$ denotes the Lagrange multipliers. By differentiating the Lagrangian L with respect to $\boldsymbol{u}$ ones get

$$\frac{\partial L(\boldsymbol{u}, \boldsymbol{\lambda})}{\partial \boldsymbol{u}} = \boldsymbol{u} - \boldsymbol{B}^T\boldsymbol{\lambda}$$

$$\frac{\partial L(\boldsymbol{u}, \boldsymbol{\lambda})}{\partial \boldsymbol{u}} = \boldsymbol{0} \Rightarrow \boldsymbol{u} = \boldsymbol{B}^T\boldsymbol{\lambda}$$

$$\boldsymbol{v} = \boldsymbol{B}\boldsymbol{u} = \boldsymbol{B}\boldsymbol{B}^T\boldsymbol{\lambda}$$

Since $\text{rank}(\boldsymbol{B}) = l$, matrix $\boldsymbol{B}\boldsymbol{B}^T$ is non-singular and the optimal solution for the Lagrange multiplier is

$$\boldsymbol{\lambda} = (\boldsymbol{B}\boldsymbol{B}^T)^{-1}\boldsymbol{v}$$

Finally, the optimal solution of the given optimization problem is

$$\boldsymbol{u} = \boldsymbol{B}^T\boldsymbol{\lambda} = \boldsymbol{B}^T(\boldsymbol{B}\boldsymbol{B}^T)^{-1}\boldsymbol{v}$$

■

A.3.2 The Least Square Problem

Lemma A6 (Pseudoinverse - the least square problem)**.** *The problem*

$$\min_u \|\boldsymbol{W}(\boldsymbol{u} - \boldsymbol{u}_d)\|_2$$

$$\textit{subject to } \boldsymbol{B}\boldsymbol{u} = \boldsymbol{v}$$

where $\boldsymbol{u}_d \in \mathbb{R}^r$ *is an arbitrary vector. The solution of this problem is [120]*

$$\boldsymbol{u} = \boldsymbol{F}\boldsymbol{u}_0 + \boldsymbol{G}\boldsymbol{v}$$

where

$$\boldsymbol{F} = \boldsymbol{I} - \boldsymbol{G}\boldsymbol{B}$$
$$\boldsymbol{G} = \boldsymbol{W}^{-1}(\boldsymbol{B}\boldsymbol{W}^{-1})^{+}$$

Proof. The substitution $\boldsymbol{e} = \boldsymbol{W}(\boldsymbol{u} - \boldsymbol{u}_d)$ yields $\boldsymbol{u} = \boldsymbol{u}_d + \boldsymbol{W}^{-1}\boldsymbol{e}$ and gives the equivalent minimum norm problem formulation

$$\min_{e} \|\boldsymbol{e}\|_2$$
$$\text{subject to } \boldsymbol{B}(\boldsymbol{u}_d + \boldsymbol{W}^{-1}\boldsymbol{e}) = \boldsymbol{v} \Leftrightarrow (\boldsymbol{B}\boldsymbol{W}^{-1})\boldsymbol{e} = \boldsymbol{v} - \boldsymbol{B}\boldsymbol{u}_d$$

Again, using Lemma A5 we get

$$\boldsymbol{e} = (\boldsymbol{B}\boldsymbol{W}^{-1})^{\dagger}(\boldsymbol{v} - \boldsymbol{B}\boldsymbol{u}_d) \;\Rightarrow\; \boldsymbol{u} = (\boldsymbol{I} - \boldsymbol{W}^{-1}(\boldsymbol{B}\boldsymbol{W}^{-1})^{\dagger}\boldsymbol{B})\boldsymbol{u}_d + \boldsymbol{W}^{-1}(\boldsymbol{B}\boldsymbol{W}^{-1})^{\dagger}\boldsymbol{v}$$

■

A.4 Cosine Direction Matrix for Attitude Modelling

A.4.1 Definitions

The basic three-axis attitude transformation is based on the direction cosine matrix. Any attitude transformation in space is actually converted to this essential form [259]. In Figure A.1, the axes 1, 2, and 3 are unit vectors defining an orthogonal, right-handed triad. This triad is chosen as the reference inertial frame. Next, a similar orthogonal triad is attached to the center of mass of a moving body, defined by the unit vectors $\boldsymbol{u}$, $\boldsymbol{v}$, and $\boldsymbol{w}$.

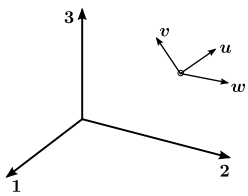


Figure A.1 – Definition of the orientation of the spacecraft axes $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ in the reference frame $\mathbf{1}, \mathbf{2}, \mathbf{3}$.

In the context of Fig. A.1, the matrix $\boldsymbol{A}$ is defined as follows:

$$\boldsymbol{A} = \begin{bmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{bmatrix}$$

In this matrix, u_1, u_2, u_3 are the components of the unit vector $\boldsymbol{u}$ along the three axes 1,2,3 of the reference orthogonal system: $\boldsymbol{u} = [u_1\ u_2\ u_3]^T$. In a similar way, $\boldsymbol{v}$ and $\boldsymbol{w}$ have components v_1, v_2, v_3 and w_1, w_2, w_3 along the same reference axes: $\boldsymbol{v} = [v_1\ v_2\ v_3]^T$ and $\boldsymbol{w} = [w_1\ w_2\ w_3]^T$. The direction cosine matrix $\boldsymbol{A}$, also called the attitude matrix has the important property of mapping vectors from the reference frame to the body frame. Suppose that a vector $\boldsymbol{a}$ has components a_1, a_2, a_3 in the reference frame: $\boldsymbol{a} = [a_1\ a_2\ a_3]^T$. The following matrix vector

multiplication expresses the components of the vector $\boldsymbol{a}$ in the body frame

$$\boldsymbol{A}\boldsymbol{a} = \begin{bmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \boldsymbol{a}_b$$

where $\boldsymbol{a}_b$ is the vector $\boldsymbol{a}$ mapped into the body frame. Since $\boldsymbol{u}$ is a unit vector, it follows that the scalar product $\vec{\boldsymbol{u}}.\vec{\boldsymbol{a}}$ is the component a_u of the vector $\boldsymbol{a}$ along the unit vector $\boldsymbol{u}$. By the same reasoning, the components of the vector $\boldsymbol{a}$ on the remaining unit vectors of the body triad are a_v and a_w.

A.4.2 Basic Properties

Some basic properties of the matrix $\boldsymbol{A}$ may be stated as follows:

- Each of its elements is the cosine of the angle between a body unit vector and a reference axis; its name is derived from this property.
- Each of the vectors $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ are vectors with unit length, hence

$$\sum_{i=1}^{3} u_i^2 = 1, \quad \sum_{i=1}^{3} v_i^2 = 1, \quad \sum_{i=1}^{3} w_i^2 = 1$$

- The unit vectors $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ are orthogonal to each other, hence

$$\sum_{i=1}^{3} u_i v_i = 0, \quad \sum_{i=1}^{3} u_i w_i = 0, \quad \sum_{i=1}^{3} v_i w_i = 0$$

- These relationships lead to the useful identity $\boldsymbol{A}\boldsymbol{A}^T = I$ and thus $\boldsymbol{A}^T = \boldsymbol{A}^{-1}$. Of course, transposition of a matrix is a much simpler process than inversion of the same matrix.
- It is well known that $\det(\boldsymbol{A}) = \boldsymbol{u} \cdot (\boldsymbol{v} \times \boldsymbol{w})$. Since $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ form a cubic orthogonal triad, it follows that $\det(\boldsymbol{A}) = 1$. Thus,

$$\boldsymbol{a} = \boldsymbol{A}^T \boldsymbol{a}_b$$

- Finally, $\boldsymbol{A}$ is a proper real orthogonal matrix. Such a matrix transformation preserves the lengths of vectors and also the angles between them, and thus represents a rotation. The product of two proper real orthogonal matrices $\boldsymbol{A} = \boldsymbol{A}_2\boldsymbol{A}_1$ is the result of two successive rotations, first by $\boldsymbol{A}_1$ and then by $\boldsymbol{A}_2$. This property is useful in modelling spacecraft attitude since a chain of successive rotations is common.

A.5 Quaternions

A.5.1 Definition

The quaternion basic definition is a consequence of the properties of the direction cosine matrix $\boldsymbol{A}$. It is shown by linear algebra that a proper real orthogonal 3×3 matrix has at least one

eigenvector with eigenvalue of unity. This means that, since one of the eigenvalues $\lambda_i, i = 1, 2, 3$ is unity, the eigenvector is unchanged by the matrix $\boldsymbol{A}$:

$$\boldsymbol{A}\boldsymbol{v}_1 = \mathbf{1}.\boldsymbol{v}_1$$

The eigenvector $\boldsymbol{v}_1$ has the same components along the body axes and along the reference frame axes (see Fig. A.1 for an illustration). The existence of such an eigenvector is the analytical demonstration of Euler's famous theorem about rotational displacement [259]: "*The most general displacement of a rigid body with one point fixed is a rotation about some axis*". In this case, the rotation is about the eigenvector $\boldsymbol{v}_1$. Any attitude transformation in space by consecutive rotations about the three orthogonal unit vectors of the coordinate system can thus be achieved by a single rotation about the eigenvector with unity eigenvalue, i.e., $\boldsymbol{v}_1$.
The quaternion is defined as a vector in the following way

$$\boldsymbol{q} = q_0 + q_1\vec{i} + q_2\vec{j} + q_3\vec{k}$$

where the unit vectors $\vec{i}, \vec{j}$, and $\vec{k}$ satisfy the following equalities:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ \vec{i}.\vec{j} = -\vec{j}.\vec{i} &= \vec{k} \\ \vec{j}.\vec{k} = -\vec{k}.\vec{j} &= \vec{i} \\ \vec{k}.\vec{i} = -\vec{i}.\vec{k} &= \vec{j} \end{aligned}$$

In the definition of the quaternion $\boldsymbol{q}$, q_0 is a scalar. These equations show that the order of multiplication is important. The conjugate of $\boldsymbol{q}$ is also define as

$$\boldsymbol{q}^* = q_0 - q_1\vec{i} - q_2\vec{j} - q_3\vec{k}$$

A.5.2 Conversion from Quaternion to Euler Angles

Consider the attitude be represented by a unit quaternion $\boldsymbol{q} = (q_0, q_1, q_2, q_3)$, then the mapping from a unit quaternion to a set of Euler (3,2,1) angles is given by [59]

$$\begin{bmatrix} \varphi \\ \theta \\ \psi \end{bmatrix} = \begin{bmatrix} \text{atan2}\left(2(q_0q_1 + q_2q_3), 1 - 2(q_1^2 + q_2^2)\right) \\ \arcsin\left(2(q_0q_2 - q_3q_1)\right) \\ \text{atan2}\left(2(q_0q_3 + q_1q_2), 1 - 2(q_2^2 + q_3^2)\right) \end{bmatrix}$$

where

$$\text{atan2}(y, x) = \begin{cases} \arctan\left(\frac{y}{x}\right) & x > 0 \\ \arctan\left(\frac{y}{x}\right) + \pi & y \geq 0, x < 0 \\ \arctan\left(\frac{y}{x}\right) - \pi & y < 0, x < 0 \\ +\frac{\pi}{2} & y > 0, x = 0 \\ -\frac{\pi}{2} & y < 0, x = 0 \\ \text{undefined} & y = 0, x = 0 \end{cases}$$

A.5.3 Quaternion Product

Quaternion product $\odot$ between quaternions $\boldsymbol{q}^a \in \mathbb{H}$ and $\boldsymbol{q}^b \in \mathbb{H}$ is defined as follows [59]

$$\begin{aligned}
\boldsymbol{q}^a \odot \boldsymbol{q}^b &= \begin{bmatrix} q_0^a q_0^b - (\boldsymbol{q}_{1:3}^a)^T \boldsymbol{q}_{1:3}^b \\ q_0^a \boldsymbol{q}_{1:3}^b + q_0^b \boldsymbol{q}_{1:3}^a - \boldsymbol{q}_{1:3}^a \times \boldsymbol{q}_{1:3}^b \end{bmatrix} \\
&= \begin{bmatrix} q_0^a & -(\boldsymbol{q}_{1:3}^a)^T \\ \boldsymbol{q}_{1:3}^a & +q_0^a \boldsymbol{I} + C(\boldsymbol{q}_{1:3}^a) \end{bmatrix} \begin{bmatrix} q_0^b \\ \boldsymbol{q}_{1:3}^b \end{bmatrix} \\
&= \begin{bmatrix} q_0^b & -(\boldsymbol{q}_{1:3}^b)^T \\ \boldsymbol{q}_{1:3}^b & +q_0^b \boldsymbol{I} + C(\boldsymbol{q}_{1:3}^b) \end{bmatrix} \begin{bmatrix} q_0^a \\ \boldsymbol{q}_{1:3}^a \end{bmatrix}
\end{aligned}$$

where the skew-symmetric *cross product matrix* function $C(\cdot) : \mathbb{R}^3 \to \mathbb{R}^{3\times 3}$ of $\boldsymbol{x} \in \mathbb{R}^3$ is defined by

$$C(\boldsymbol{x}) = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix}$$

Note that quaternion product is non-commutative.

Appendix B

Hypothesis Testing

The task of the statistical hypothesis testing of the residual is to determine the presence and the time occurrence of a fault in the system. The fault indicating residual signal can be generated by different ways, see Section 1.3. The decision is based on accepting or rejecting one of the following two possible hypotheses:

- H_0 : normal operation (the system is fault-free),
- H_1 : abnormal operation (the system is faulty).

One can ask, how to choose between these two hypotheses with a given risk. Let $p(r|H_0)$ and $p(r|H_1)$ be the conditional PDF (Probability Density Function) associated with the residual r under the condition of H_0 and H_1, respectively. Consider a fixed decision threshold chosen based on a priori knowledge of the decision problem, then the decision process can result in four possible scenarios, see Table B.1.

	H_0 declared	H_1 declared
H_0 is true	right decision	false alarm P_f
H_1 is true	non-detection P_{nd}	right decision

Table B.1 – Decision situations in a two-hypothesis test

A hypothesis test is then a rule that, for a given measurement, makes a decision as to which hypothesis best "explains" the data. Figure B.1 illustrates the overlap of the two PDFs and the selected threshold.

B.1 Wald's Sequential Probability Ratio Test

A Sequential Probability Ratio Test (SPRT), also known as Wald's sequential test, is a diagnostic algorithm generally used when the residual of the system follows a Gaussian distribution. Non-sequential diagnostic tests are dependent on the number of observed samples being tested. In practice, a moving window is used on the residual. For Wald's sequential test, the width of the sample size is not fixed a priori, but depends upon the data that have been already observed. A decision is made as soon as there are enough observations in the actual step so that error

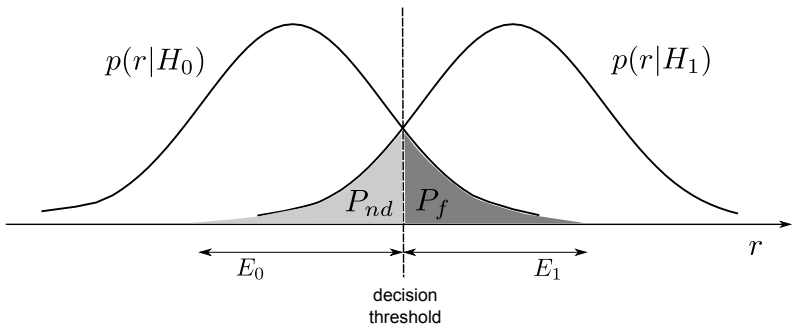


Figure B.1 – Definition of the probability of non-detection and false alarm and the decision threshold

probabilities are inferior to set values. These values are the non-detection P_{nd} and false alarm P_f probabilities. The sequential decision-making theory was developed by Abraham Wald in his famous book [287] as a statistical tool for sequential hypothesis testing. A good survey on hypothesis testing can be found in [10].

B.1.1 Decision Test

Assume that $r(k)$ is a random variable, and S_1 and S_2 are two decision thresholds ($S_1 < S_2$) such that:[1]

- **Situation No.1:** if $r(k) \leq S_1$, then H_0 is accepted;
- **Situation No.2:** if $S_1 < r(k) < S_2$, then no decision is adopted;
- **Situation No.3:** if $r(k) \geq S_2$, then H_1 is accepted.

Wald's sequential test relies on the connection of the two decision thresholds S_1 and S_2 with the probability of non-detection P_{nd} and false alarm P_f, defined by:

$$P_{nd} = \text{probability}(H_0 \text{ is declared}|H_1 \text{ true})$$

$$P_f = \text{probability}(H_1 \text{ is declared}|H_0 \text{ true})$$

The detection probability, denoted as P_d, is defined by:

$$P_d = \text{probability}(H_1 \text{ is declared}|H_1 \text{ true})$$

B.1.2 Calculation of the Decision Thresholds

Assume that the probability density functions associated with H_0 and H_1 have been determined and are noted as $p(r(k)|H_0)$ and $p(r(k)|H_1)$, where $r(k)$ is the residual at the time instant k. Then, the probability P_f, P_{nd} and P_d are mathematically given by:

$$P_{nd} = \int_{E_0} p(r(k)|H_1)dr(k) \tag{B.1}$$

[1] A scalar discrete time residual signal $r(k)$ is considered.

$$P_f = \int_{E_1} p(r(k)|H_0)dr(k) \tag{B.2}$$

$$P_d = \int_{E_1} p(r(k)|H_1)dr(k) = 1 - P_{nd} \tag{B.3}$$

and the likelihood ratio $\lambda(k)$ for Wald's sequential test is given by:

$$\lambda(k) = \frac{p\left(r(1), r(2), \ldots, r(k)|H_1\right)}{p\left(r(1), r(2), \ldots, r(k)|H_0\right)} \tag{B.4}$$

Situation No.1

In this case, it is assumed that at sample k the system is normal functioning ($r(k) \leq S_1$). The threshold is determined by considering the extreme case when the likelihood ratio $\lambda(k)$ is equal to A. Then from (B.4), for all samples from 1 to k, the following yields:

$$p(r(k)|H_1) = Ap(r(k)|H_0) \tag{B.5}$$

Now, integrating (B.5) over the space E_0, it follows that

$$\int_{E_0} p(r(k)|H_1)dr(k) = A\int_{E_0} p(r(k)|H_0)dr(k) \tag{B.6}$$

Considering (B.1) and (B.2), it yields

$$P_{nd} = A(1 - P_f) \tag{B.7}$$

and thus

$$A = \frac{P_{nd}}{1 - P_f} \tag{B.8}$$

Situation No.2

Here, the case when no decision is adopted ($S_1 < r(k) < S_2$) is considered. Supposing that samples $r(i), i = 1, ..., k$ are independent of each other, then (B.4) can be rewritten as follows:

$$\lambda(k) = \frac{p(r(1)|H_1)p(r(2)|H_1)\ldots p(r(k)|H_1)}{p(r(1)|H_0)p(r(2)|H_0)\ldots p(r(k)|H_0)} \tag{B.9}$$

or alternatively

$$\lambda(k) = \prod_{i=1}^{k} \lambda^{\circ}(i), \text{ where } \lambda^{\circ}(i) = \prod_{i=1}^{k} \frac{p(r(i)|H_1)}{p(r(i)|H_0)} \tag{B.10}$$

Situation No.3

It is assumed that at sample k the system is faulty ($r(k) \leq S_1$). Similarly as in situation No.1, the limit case $\lambda(k) = B$ is considered. From (B.4), for all samples from 1 to k, it follows that:

$$p(r(k)|H_1) = Bp(r(k)|H_0) \tag{B.11}$$

and integrating (B.11) over the space E_1, it follows that

$$\int_{E_1} p(r(k)|H_1)dr(k) = B\int_{E_1} p(r(k)|H_0)dr(k) \tag{B.12}$$

Thus, considering (B.1) and (B.2), it yields

$$P_d = BP_f \tag{B.13}$$

and from (B.3), it follows:

$$B = \frac{1 - P_{nd}}{P_f} \tag{B.14}$$

B.1.3 Wald's Test for the Mean Value

Let r be a Gaussian random variable regardless of the operation mode of the system (faulty or fault-free). The idea of this test is to find out whether the statistical mean of this signal has been changed.

Let be assumed that under hypothesis H_0, r has a mean value μ_0 and a variance σ^2, and under the hypothesis H_1, r has a mean value μ_1 and variance σ^2, i.e.,

$$E\{r\} = \mu_0 \text{ under } H_0 \tag{B.15}$$

$$E\{r\} = \mu_1 \text{ under } H_1 \tag{B.16}$$

$$E\left\{(r-\mu_0)(r-\mu_0)^T\right\} = E\left\{(r-\mu_1)(r-\mu_1)^T\right\} = \sigma^2 \tag{B.17}$$

The probability density function are then expressed as:

$$p(r(k)|H_1) = \frac{1}{\sigma\sqrt{2\pi}}\exp\left\{-\frac{1}{2\sigma^2}(r(k)-\mu_1)^2\right\} \tag{B.18}$$

$$p(r(k)|H_0) = \frac{1}{\sigma\sqrt{2\pi}}\exp\left\{-\frac{1}{2\sigma^2}(r(k)-\mu_0)^2\right\} \tag{B.19}$$

The expression of the likelihood ratio given by (B.10) for the mean value becomes (the index "m" indicates the mean value):

$$\begin{aligned}\lambda^m(k) &= \prod_{i=1}^{k}\exp\left\{-\frac{1}{2\sigma^2}(r(i)-\mu_1)^2 + \frac{1}{2\sigma^2}(r(i)-\mu_0)^2\right\} = \\ &= \prod_{i=1}^{k}\exp\left\{-\frac{1}{2\sigma^2}\left[(r(i)^2 - 2r(i)\mu_1 + \mu_1^2) - (r(i)^2 - 2r(i)\mu_0 + \mu_0^2)\right]\right\} = \\ &= \prod_{i=1}^{k}\exp\left\{-\frac{1}{2\sigma^2}\left(\mu_1^2 - \mu_0^2\right) + \frac{1}{\sigma^2}\left(\mu_1 - \mu_0\right)r(i)\right\}\end{aligned} \tag{B.20}$$

Simplifying (B.20) results in

$$\lambda^m(k) = \exp\left\{-\frac{k}{2\sigma^2}(\mu_1^2 - \mu_0^2) + \frac{1}{\sigma^2}(\mu_1 - \mu_0)\sum_{i=1}^{k} r(i)\right\} \tag{B.21}$$

The sequential Wald's test for the mean value can be now written as

$$A \leq \lambda^m(k) \leq B \tag{B.22}$$

Substituting (B.21) into (B.22) yields

$$A \leq \exp\left\{-\frac{k}{2\sigma^2}(\mu_1^2 - \mu_0^2) + \frac{1}{\sigma^2}(\mu_1 - \mu_0)\sum_{i=1}^{k} r(i)\right\} \leq B \tag{B.23}$$

Applying natural logarithm

$$\ln(A) \leq \frac{\mu_1 - \mu_0}{\sigma^2}\left\{-\frac{k}{2}(\mu_1 + \mu_0) + \sum_{i=1}^{k} r(i)\right\} \leq \ln(B) \tag{B.24}$$

Finally after some tedious calculations the following holds

$$\frac{\sigma^2}{\mu_1 - \mu_0}\ln(A) + \frac{k}{2}(\mu_1 + \mu_0) \leq \sum_{i=1}^{k} r(i) \leq \frac{\sigma^2}{\mu_1 - \mu_0}\ln(B) + \frac{k}{2}(\mu_1 + \mu_0) \tag{B.25}$$

where A and B are fixed as given in (B.1) and (B.2) using the probabilities P_{nd} and P_f.

B.1.3.1 Graphical Interpretation

The graphical interpretation of the sequential Wald's decision test for the mean value is depicted in Figure B.2. The time varying thresholds are defined according to

$$g_1(k) = \frac{\sigma^2}{\mu_1 - \mu_0}\ln(A) + \frac{(\mu_1 + \mu_0)}{2}k \tag{B.26}$$

$$g_2(k) = \frac{\sigma^2}{\mu_1 - \mu_0}\ln(B) + \frac{(\mu_1 + \mu_0)}{2}k \tag{B.27}$$

These equations represent two parallel lines with gradient $\frac{\mu_1+\mu_0}{2}$ and origin in $\frac{\sigma^2}{\mu_1-\mu_0}\ln(A)$ for $g_1(k)$, and in $\frac{\sigma^2}{\mu_1-\mu_0}\ln(B)$ for $g_2(k)$, respectively.

B.1.3.2 Modification to the Change of the Mean

By subtracting $k\mu_0$ from (B.25), the following yields

$$\frac{\sigma^2}{\mu_1-\mu_0}\ln(A) + \frac{k}{2}(\mu_1 - \mu_0) \leq \sum_{i=1}^{k}(r(i) - \mu_0) \leq \frac{\sigma^2}{\mu_1-\mu_0}\ln(B) + \frac{k}{2}(\mu_1 - \mu_0) \tag{B.28}$$

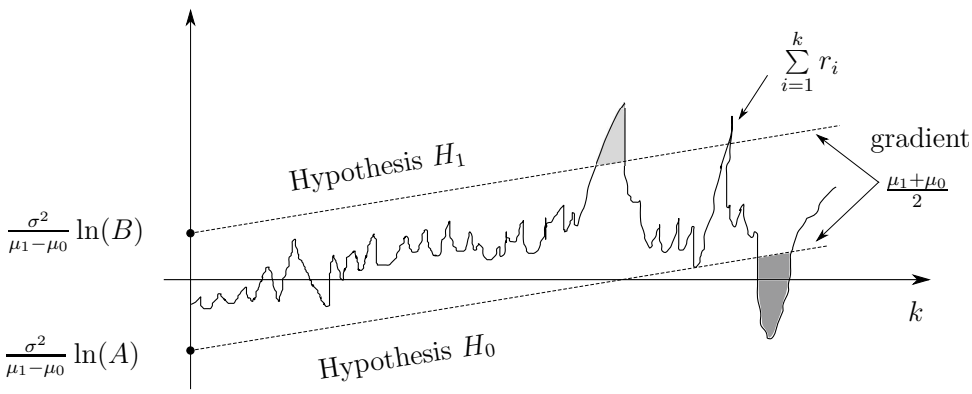


Figure B.2 – Graphical interpretation of the Wald's decision test for the mean value

Introducing a new parameter $\Delta\mu = \mu_1 - \mu_0$, (B.28) can be rewritten as

$$\frac{\sigma^2}{\Delta\mu}\ln(A) + k\frac{\Delta\mu}{2} \leq \sum_{i=1}^{k}(r(i) - \mu_0) \leq \frac{\sigma^2}{\Delta\mu}\ln(B) + k\frac{\Delta\mu}{2} \tag{B.29}$$

where it is required that $\Delta\mu > 0$, therefore $\Delta\mu = |\mu_1 - \mu_0|$ has to be considered.

B.1.4 Wald's Test for the Variance

This test deals with a change detection in the variance of the residual signal r. Let's assume that under the hypothesis H_0, r has a mean value μ and a variance σ_0^2, and under the hypothesis H_1, r has a mean value μ and variance σ_1^2, i.e.,

$$E\{r\} = \mu \text{ under } H_0 \text{ and } H_1 \tag{B.30}$$

$$E\left\{(r-\mu)(r-\mu)^T\right\} = \sigma_0^2 \text{ under } H_0 \tag{B.31}$$

$$E\left\{(r-\mu)(r-\mu)^T\right\} = \sigma_1^2 \text{ under } H_1 \tag{B.32}$$

The probability density function are then expressed as

$$p(r(k)|H_0) = \frac{1}{\sigma_0\sqrt{2\pi}}\exp\left\{-\frac{1}{2\sigma_0^2}(r(k)-\mu)^2\right\} \tag{B.33}$$

$$p(r(k)|H_1) = \frac{1}{\sigma_1\sqrt{2\pi}}\exp\left\{-\frac{1}{2\sigma_1^2}(r(k)-\mu)^2\right\} \tag{B.34}$$

The expression of the likelihood ratio given by (B.10) for the variance becomes (the index "v" indicates the variance)

$$\lambda^v(k) = \prod_{i=1}^{k}\frac{\sigma_0}{\sigma_1}\exp\left\{-\frac{1}{2}\left(\frac{1}{\sigma_1^2} - \frac{1}{\sigma_0^2}\right)(r(i)-\mu)^2\right\} \tag{B.35}$$

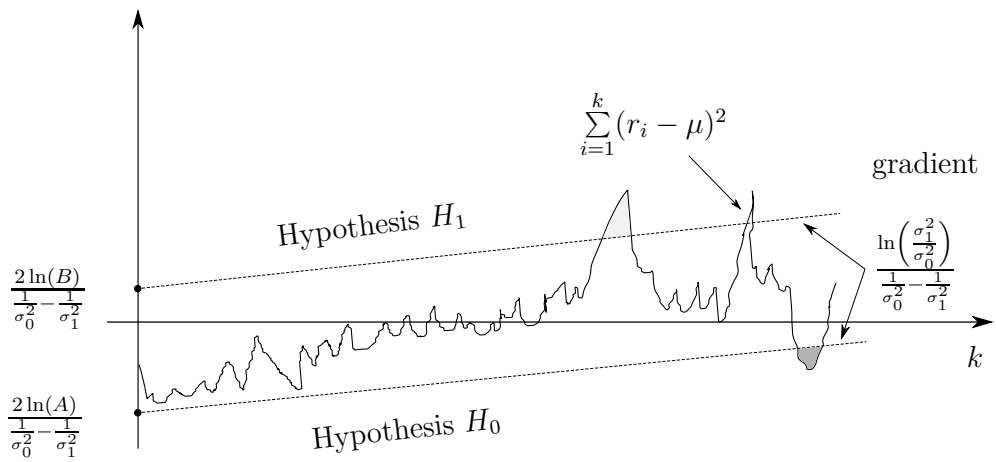


Figure B.3 – Graphical interpretation of the Wald's decision test for the variance

Simplifying (B.35) results in

$$\lambda^v(k) = \left(\frac{\sigma_0}{\sigma_1}\right)^k \exp\left\{-\frac{1}{2}\left(\frac{1}{\sigma_1^2}-\frac{1}{\sigma_0^2}\right)\sum_{i=1}^{k}(r(i)-\mu)^2\right\} \tag{B.36}$$

The sequential Wald's test for the variance can be written as:

$$A \leq \lambda^v(k) \leq B \tag{B.37}$$

Substituting (B.36) into (B.37) the following yields

$$A \leq \left(\frac{\sigma_0}{\sigma_1}\right)^k \exp\left\{-\frac{1}{2}\left(\frac{1}{\sigma_1^2}-\frac{1}{\sigma_0^2}\right)\sum_{i=1}^{k}(r(i)-\mu)^2\right\} \leq B \tag{B.38}$$

Further, applying the natural logarithm on (B.38) results in

$$\ln(A) \leq k\ln\left(\frac{\sigma_0}{\sigma_1}\right) - \frac{1}{2}\left(\frac{1}{\sigma_1^2}-\frac{1}{\sigma_0^2}\right)\sum_{i=1}^{k}(r(i)-\mu)^2 \leq \ln(B) \tag{B.39}$$

which, after some arithmetic operations, leads to

$$\frac{2\left(\ln(A)+\frac{k}{2}\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right)\right)}{\left(\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}\right)} \leq \sum_{i=1}^{k}(r(i)-\mu)^2 \leq \frac{2\left(\ln(B)+\frac{k}{2}\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right)\right)}{\left(\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}\right)} \tag{B.40}$$

where A and B are again fixed as given in (B.1) and (B.2).

B.1.4.1 Graphical Interpretation

The time varying thresholds are again defined as two parallel lines according to the following equations:

$$g_1(k) = \frac{2\ln(A)}{\left(\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}\right)} + \frac{\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right)}{\left(\frac{1}{\sigma_0^2}-\frac{1}{\sigma_1^2}\right)}k \tag{B.41}$$

$$g_2(k) = \frac{2\ln(B)}{\left(\frac{1}{\sigma_0^2} - \frac{1}{\sigma_1^2}\right)} + \frac{\ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right)}{\left(\frac{1}{\sigma_0^2} - \frac{1}{\sigma_1^2}\right)}k \tag{B.42}$$

The graphical interpretation of the sequential Wald's decision test for the variance is depicted in Figure B.3.

Remark B.1. *In order to avoid that the cumulative sum in the above mentioned methods will tend to infinity, one has to reset the cumulative sum and the thresholds as soon as a decision is taken, i.e., when H_0 or H_1 is accepted.*

B.2 Generalized Likelihood Ration Test

One of the main drawbacks of the Wald's decision test is that some knowledge is required about the residual distribution in faulty situation. In practice, once the residual generation problem is solved and the distribution of the fault-free residual is known, a Generalized Likelihood Ration (GLR) test statistic can be formed without a priori knowledge about the faulty residual distribution. Similarly as the SPRT test, the GLR test is built on the Neyman-Pearson's lemma [204].

B.2.1 Decision Test

Let's consider the two hypotheses H_0 and H_1, and assume that $r(k)$ is a random variable, then the GLR decision test can be expressed as:

- **Situation No.1:** if $r(k) \sim \mathcal{N}(\mu_0, \sigma_0)$, then H_0 is accepted;
- **Situation No.2:** if $r(k) \sim \mathcal{N}(\mu_1, \sigma_1)$, then H_1 is accepted.

where μ_0 and σ_0 are the (known) mean and standard deviation of $r(k)$ in fault-free situation, respectively and μ_1 and σ_1 are assumed to be unknown.

By the same reasoning as in the case of the Wald's test, the likelihood ratio $\lambda(k)$ between hypotheses H_0 and H_1, can be computed as in (B.4).

B.2.1.1 GLR Test for the Mean Value

This test deals with a change detection in the mean of the residual signal $r(k)$. Assume that (B.15) - (B.17) hold, i.e., the variance of the residual is assumed to be the same in both situations $\sigma^2 = \sigma_0^2 = \sigma_1^2$, then the natural logarithm of the likelihood ratio (log LR) $\lambda(k)$ is described by [60]

$$\ln \frac{p(r(k)|H_1)}{p(r(k)|H_0)} = \frac{1}{2\sigma^2}\left[(r(k) - \mu_0)^2 - (r(k) - \mu_1)^2\right] \tag{B.43}$$

where $p(r(k)|H_1)$ and $p(r(k)|H_0)$ are given by (B.18) and (B.19), respectively.

In case of N samples of r, $r(k)$, $k = 1, \ldots, N$, are available, the log LR is defined by [60]

$$S_1^N = \sum_{i=1}^{N} \ln \frac{p(r(i)|H_1)}{p(r(i)|H_0)} = \frac{1}{2\sigma^2} \sum_{i=1}^{N} \left[(r(i) - \mu_0)^2 - (r(i) - \mu_1)^2 \right] \tag{B.44}$$

$$= \frac{\mu_1 - \mu_0}{\sigma^2} \sum_{i=1}^{N} \left(r(i) - \frac{\mu_1 + \mu_0}{2} \right) \tag{B.45}$$

In practice, μ_1 is unknown. Thus, μ_1 is replaced by its maximum likelihood estimate. The maximum likelihood estimate $\hat{\mu}_1$ of μ_1 is an estimate achieved under the cost function that the LR is maximized, i.e., $\max_{\mu_1} S_1^N \Rightarrow \frac{\partial S_1^N}{\partial \mu_1} = 0$, which yields to

$$\hat{\mu}_1 = \arg\max_{\mu_1} S_1^N = \bar{r} = \frac{1}{N} \sum_{i=1}^{N} r(i) \tag{B.46}$$

where $\bar{r}$ is the mean value of the residual r, i.e., $\bar{r} = \frac{1}{N} \sum_{i=1}^{N} r(i)$. With (B.46) the LR is maximised [60]. It can be seen that the maximum likelihood estimate of μ_1 is in fact the estimate of the mean value $\bar{r}$. Substituting $\hat{\mu}_1$ for μ_1 in (B.44) gives the GLR algorithm for the mean value

$$S_1^N = \frac{1}{2\sigma^2 N} \left(\sum_{i=1}^{N} (r(i) - \mu_0) \right)^2 \tag{B.47}$$

B.2.1.2 GLR Test for the Variance

This test deals with a change detection in the variance of the residual signal r. To proceed, assume that (B.30) - (B.32) hold, i.e., the mean of the residual is assumed to be the same for both situations $\mu = \mu_0 = \mu_1$, and the log LR for the first N samples is given by [10, 60]

$$S_1^N = \sum_{i=1}^{N} \ln \frac{p(r(i)|H_1)}{p(r(i)|H_0)} = N \ln \frac{\sigma_0}{\sigma_1} + \frac{1}{2\sigma_0^2} \sum_{i=1}^{N} (r(i) - \mu)^2 - \frac{1}{2\sigma_1^2} \sum_{i=1}^{N} (r(i) - \mu)^2 \tag{B.48}$$

where $p(r(i)|H_1)$ and $p(r(i)|H_0)$ are given by (B.33) and (B.34), respectively. Since σ_1^2 is unknown, its maximum estimate $\hat{\sigma}_1$ is considered, i.e., $\max_{\sigma_1} S_1^N \Rightarrow \frac{\partial S_1^N}{\partial \sigma_1} = 0$, which yields to

$$\hat{\sigma}_1^2 = \arg\max_{\sigma_1} S_1^N = \frac{1}{N} \sum_{i=1}^{N} (r(i) - \mu)^2 \tag{B.49}$$

Substituting (B.49) into (B.48) gives the GLR algorithm for the variance

$$S_1^N = N \ln(\sigma_0) - \frac{N}{2} \left[1 + \ln \left(\frac{1}{N} \sum_{i=1}^{N} (r(i) - \mu)^2 \right) \right] + \frac{1}{2\sigma_0^2} \sum_{i=1}^{N} (r(i) - \mu)^2 \tag{B.50}$$

Remark B.2. *Another algorithm exists in the literature to test the change in variance according*

to the χ^2 statistics. The statistics

$$S_1^N = \frac{(N-1)s^2}{\sigma_0^2}, \qquad s^2 = \frac{\sum_{i=1}^{N}(r(i)-\bar{r})^2}{N-1} \tag{B.51}$$

has a standard χ^2 distribution with the degree of freedom equal to $N-1$. Thus, for a given significance level α, the threshold is determined by

$$J_{th} = \chi^2_{\alpha,\gamma}, \quad prob\{S_1^N > \chi^2_{\alpha,\gamma}\} = \alpha \tag{B.52}$$

where $\chi^2_{\alpha,\gamma}$ is given by the standard χ^2 distribution table corresponding to the significance level α and degree of freedom γ equal to $\gamma = N-1$. This algorithm was used for the decision test in [90].

B.2.2 On-line Realization

The above presented GLR algorithms can be realized on a fixed sliding window $N_d \in \mathbb{Z}^+$. In this framework, (B.47) and (B.50) become

$$S^{N_d}(k) = \begin{cases} S_1^k & \text{if } k < N_d \\ S_{k-N_d+1}^k & \text{if } k \geq N_d \end{cases} \tag{B.53}$$

The sliding window N_d is introduced to tackle on-line realization aspects.

References

[1] M Abbaszadeh and H.J Marquez. LMI optimization approach to robust $h\infty$ observer design and static output feedback stabilization for discrete-time nonlinear uncertain systems. *International Journal of Robust and Nonlinear Control*, 19(3):313–340, 2009. doi: 10.1002/rnc.1310.

[2] S. Aberkane, D. Sauter, and J.C. Ponsart. Performance evaluation in active fault tolerant control systems. In *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*, pages 1573–1578, june 2005. doi: 10.1109/.2005.1469816.

[3] H. Alwi and C. Edwards. Fault detection and fault-tolerant control of a civil aircraft using a sliding-mode-based scheme. *IEEE Transactions on Control Systems Technology*, 16(3): 499–510, 2008. doi: 10.1109/TCST.2007.906311.

[4] H. Alwi and C. Edwards. Fault tolerant control using sliding modes with on-line control allocation. *Automatica*, 44(7):1859–1866, 2008. doi: 10.1016/j.automatica.2007.10.034.

[5] H. Alwi, C. Edwards, and A. Marcos. Fdi for a mars orbiting satellite based on a sliding mode observer scheme. In *Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 125–130, Nice, France, 2010. IEEE. doi: 10.1109/SYSTOL.2010.5676035.

[6] H. Alwi, C. Edwards, and C.P. Tan. *Fault detection and fault-tolerant control using sliding modes*. Springer London, 2011.

[7] J.R. Angelos, M.S. Henry, E.H. Kaufman, T.D. Lenker, and A. Kroó. Local and global Lipschitz constants. *Journal of Approximation Theory*, 46(2):137–156, 1986. ISSN 0021-9045. doi: 10.1016/0021-9045(86)90057-2.

[8] M.S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp. A tutorial on particle filters for online nonlinear/non-Gaussian bayesian tracking. *IEEE Transactions on Signal Processing*, 50(2):174–188, 2002. doi: 10.1109/78.978374.

[9] G. Basile and G. Marro. Controlled and conditioned invariant subspaces in linear system theory. *Journal of Optimization Theory and Applications*, 3(5):306–315, 1969.

[10] M. Basseville and I.V. Nikiforov. *Detection of Abrupt Changes: Theory and Application*. Prentice Hall, 1993. doi: 10.1080/00401706.1994.10485821.

[11] D. Beaty, M. Grady, L. May, and B. Gardini. Preliminary planning for an international Mars Sample Return mission. Technical report, Report of the International Mars Architecture for the Return of Samples (iMARS) Working Group, 2008. URL `http://mepag.jpl.nasa.gov/reports/iMARS_FinalReport.pdf`.

[12] D.A. Belsley. *Weak Data*. Wiley Online Library, 1991.

[13] A. Bemporad, A. Casavola, and E. Mosca. Nonlinear control of constrained linear systems via predictive reference management. *IEEE Transactions on Automatic Control*, 42(3): 340–349, 1997. doi: 10.1109/9.557577.

[14] S. Bhattacharyya. Observer design for linear systems with unknown inputs. *IEEE Transactions on Automatic Control*, 23(3):483–484, 1978. doi: 10.1109/TAC.1978.1101758.

[15] G. Biswas, M.O. Cordier, J. Lunze, L. Trave-Massuyes, and M. Staroswiecki. Diagnosis of complex systems: Bridging the methodologies of the fdi and dx communities. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 34(5):2159–2162, 2004.

[16] M Blanke. *Fault-tolerant control systems*. Springer, 1999.

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

[18] M. Blanke, M. Staroswiecki, and N. E. Wu. Concepts and methods in fault-tolerant control. In *American Control Conference*, volume 4, pages 2606–2620. IEEE, 2001.

[19] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag Berlin Heidelberg, 2nd edition, 2006.

[20] J. Boada, C. Prieur, S. Tarbouriech, C. Pittet, and C. Charbonnel. Multi-saturation anti-windup structure for satellite control. In *Proc. American Control Conference*, pages 5979–5984, Baltimore, USA, June 2010. doi: 10.1109/ACC.2010.5531254.

[21] M. Bodson. Evaluation of optimization methods for control allocation. *Journal of Guidance, Control and Dynamics*, 25(4):703–711, 2002. doi: 10.2514/2.4937.

[22] M. Bodson and J.E. Groszkiewicz. Multivariable adaptive algorithms for reconfigurable flight control. *IEEE Transactions on Control Systems Technology*, 5(2):217–229, 1997. doi: 10.1109/87.556026.

[23] J. Bokor and G. Balas. Detection filter design for LPV systems - a geometric approach. *Automatica*, 40(3):511–518, 2004. doi: 10.1016/j.automatica.2003.11.003.

[24] J. Bokor and Z. Szabó. Fault detection and isolation in nonlinear systems. *Annual Reviews in Control*, 33(2):113–123, 2009. doi: 10.1016/j.arcontrol.2009.09.001.

[25] Kenneth A Bordignon. *Constrained control allocation for systems with redundant control effectors*. PhD thesis, Virginia Polytechnic Institute and State University, 1996.

[26] J. Boskovic and R. Mehra. Failure detection, identification and reconfiguration in flight control. pages 129–167. Springer, 2003.

[27] J.D. Boskovic and R.K. Mehra. A multiple model-based reconfigurable flight control system design. In *Proceedings of the 37th IEEE Conference on Decision and Control*, volume 4, pages 4503–4508. IEEE, 1998.

[28] J.D. Boskovic and R.K. Mehra. Stable multiple model adaptive flight control for accommodation of a large class of control effector failures. In *Proceedings of the American Control Conference*, volume 3, pages 1920 –1924 vol.3, 1999. doi: 10.1109/ACC.1999.786187.

[29] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan. *Linear matrix inequalities in system and control theory*, volume 15. Society for Industrial and Applied Mathematics, 1994.

[30] J.M. Buffington and D.F. Enns. Lyapunov stability analysis of daisy chain control allocation. *Journal of Guidance, Control, and Dynamics*, 19(6), 1996. doi: 10.2514/3.21776.

[31] J. J. Burken, P. Lu, Z. Wu, and C. Bahm. Two reconfigurable flight-control design methods: Robust servomechanism and control allocation. *Journal of Guidance, Control, and Dynamics*, 24(3):482–493, 2001.

[32] A.K. Caglayan, S.M. Allen, and K. Wehmuller. Evaluation of a second generation reconfiguration strategy for aircraft flight control systems subjected to actuator failure/surface damage. In *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, NAECON*, pages 520–529. IEEE, 1988.

[33] A. J. Calise, S. Lee, and M. Sharma. Development of a reconfigurable flight control law for the x-36 tailless fighter aircraft. In *AIAA guidance, navigation, and control conference*, 2000.

[34] C. Cazaux, F. Naderi, C. Whetsel, D. Beaty, B. Gershman, R. Kornfeld, B. Mitcheltree, and B. Sackheim. The NASA/CNES Mars Sample Return - a status report. *Acta Astronautica*, 54(8):601–617, 2004. ISSN 0094-5765. doi: 10.1016/j.actaastro.2003.07.001.

[35] A. Chamseddine, C. Join, and D. Theilliol. Trajectory planning/re-planning for satellite systems in rendezvous mission in the presence of actuator faults based on attainable efforts analysis. *International Journal of Systems Science*, 46(4):690–701, 2015. doi: 10.1080/00207721.2013.797034.

[36] P.R. Chandler. Self-repairing flight control system reliability and maintainability program executive overview. In *Proceeding of the IEEE National Aerospace and Electronics Conference*, pages 586–590, 1984.

[37] F. Chatelin. *Spectral Approximation of Linear Operators*. Academic Press. Society for Industrial and Applied Mathematics, New York, 1983.

[38] J. Chaudenson, D. Beauvois, S. Bennani, M. Ganet-Schoeller, and G. Sandou. Dynamics modeling and comparative robust stability analysis of a space launcher with constrained inputs. In *12th European Control Conference*, pages 353–358, Zurich, Switzerland, 2013.

[39] J. Chen and R. Patton. *Robust model-based fault diagnosis for dynamic systems*. Kluwer Academic Publishers, Dordrecht, 1999. doi: 10.1007/978-1-4615-5149-2.

[40] J. Chen and R.J. Patton. Optimal filtering and robust fault diagnosis of stochastic systems with unknown disturbances. In *IEE Proceedings - Control Theory and Applications*, volume 143, pages 31–36. IET, 1996.

[41] W. Chen and M. Saif. An iterative learning observer-based approach to fault detection and accommodation in nonlinear systems. In *Proceedings of the 40th IEEE Conference on Decision and Control*, volume 5, pages 4469–4474, 2001. doi: 10.1109/.2001.980906.

[42] W. Chen and M. Saif. A robust iterative learning observer-based fault diagnosis of time delay nonlinear systems. In *Proceedings of the 15th Triennial World Congress of IFAC*, 2002.

[43] W. Chen and M. Saif. Unknown input observer design for a class of nonlinear systems: an LMI approach. In *Proc. of American Control Conference*, pages 834–838, Minneapolis, USA, 2006.

[44] W. Chen and M. Saif. Observer-based fault diagnosis of satellite systems subject to time-varying thruster faults. *Journal of Dynamic Systems, Measurement and Control*, 129(3): 352–356, 2007. doi: 10.1115/1.2719773.

[45] M. Chilali and P. Gahinet. h_∞ design with pole placement constraints: An LMI approach. *IEEE Transactions on Automatic Control*, 41(3):358–367, 1996. doi: 10.1109/9.486637.

[46] J.W. Choi. A simultaneous assignment methodology of right/left eigenstructures. *IEEE Transactions on Aerospace and Electronic Systems*, 34(2):625–634, 1998. doi: 10.1109/7.670342.

[47] E. Chow and A. Willsky. Analytical redundancy and the design of robust failure detection systems. *IEEE Transactions on Automatic Control*, 29(7):603 – 614, jul 1984. ISSN 0018-9286. doi: 10.1109/TAC.1984.1103593.

[48] R.N. Clark. Instrument fault detection. *IEEE Transactions on Aerospace and Electronic Systems*, AES-14(3):456–465, may 1978. ISSN 0018-9251.

[49] W.H. Clohessy and R.S. Wiltshire. Terminal guidance system for satellite rendezvous. *Journal of the Aerospace Science*, 27(9):653–658, 1960. doi: 10.2514/8.8704.

[50] J. L. Crassidis and J. L. Junkins. *Optimal estimation of dynamic systems*, volume 24. Chapman & Hall, 2011.

[51] NB Crosby. Solar extreme events 2005–2006: Effects on near-earth space systems and interplanetary systems. *Advances in Space Research*, 43(4):559–564, 2009.

[52] M. Daigle, X. Koutsoukos, and G. Biswas. Multiple fault diagnosis in complex physical systems. In *Proceedings of the 17th International Workshop on Principles of Diagnosis (DX 06)*, 2006.

[53] L. A. D'Amario, W. E. Bollman, W. J. Lee, R. B. Roncoli, J. C. Smith, S. B. Ramachandra, and B. F. Raymond. Mars orbit rendezvous strategy for the mars 2003/2005 Sample Return Mission. In *AIAA/AAS Astrodynamics Specialist Conference*, Girdwood, USA, August 1999.

[54] V. Dardinier-Maron, F. Hamelin, and H. Noura. A fault-tolerant control design against major actuator failures: application to a three-tank system. In *Conference on Decision and Control*, volume 4, pages 3569–3574. IEEE, 1999.

[55] M. Darouach, M. Zasadzinski, and S. J. Xu. Full-order observers for linear systems with unknown inputs. *IEEE Transactions on Automatic Control*, 39(3):606–609, 1994. doi: 10.1109/9.280770.

[56] J. De Kleer and B.C. Williams. Diagnosing multiple faults. *Artificial intelligence*, 32(1): 97–130, 1987. doi: 10.1016/0004-3702(87)90063-4.

[57] C. De Persis and A. Isidori. A geometric approach to nonlinear fault detection and isolation. *IEEE Transactions on Automatic Control*, 46(6):853 –865, jun 2001. ISSN 0018-9286. doi: 10.1109/9.928586.

[58] A. Dehghani, B. D. Anderson, and A. Lanzon. Unfalsified adaptive control: a new controller implementation and some remarks. In *Proceedings of the European Control Conference*, pages 2–5, 2007.

[59] J. Diebel. Representing attitude: Euler angles, unit quaternions, and rotation vectors, 2006. URL `http://www.swarthmore.edu/NatSci/mzucker1/e27/diebel2006attitude.pdf`.

[60] S. X. Ding. *Model-based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools*. Springer Verlag, 1st edition, 2008.

[61] S. X. Ding, T Jeinsch, P. M. Frank, and E. L. Ding. A unified approach to the optimization of fault detection systems. *International journal of adaptive control and signal processing*, 14(7):725–745, 2000.

[62] S. X. Ding, M. Zhong, B. Tang, and P. Zhang. An LMI approach to the design of fault detection filter for time-delay LTI systems with unknown inputs. In *American Control Conference*, volume 3, pages 2137–2142. IEEE, 2001. doi: 10.1109/ACC.2001.946063.

[63] S. X. Ding, P. Zhang, P. M. Frank, and E. L. Ding. Threshold calculation using lmi-technique and its integration in the design of fault detection systems. In *Conference on Decision and Control*, volume 1, pages 469–474, Maui, HI, 2003. IEEE.

[64] X. Ding, L. Guo, and T. Jeinsch. A characterization of parity space and its application to robust fault detection. *IEEE Transactions on Automatic Control*, 44(2):337 –343, feb 1999. ISSN 0018-9286. doi: 10.1109/9.746262.

[65] A. Doucet, S.J Godsill, and C. Andrieu. *On sequential simulation-based methods for Bayesian filtering.* Univ., Department of Engineering, 1998.

[66] A. Doucet, N. De Freitas, and N. Gordon. *Sequential Monte Carlo methods in practice.* Springer Verlag, 2001.

[67] J. Doyle. Analysis of feedback systems with structured uncertainties. In *IEE Proceedings D. Control Theory and Applications*, volume 129, pages 242–250. IET, 1982.

[68] G.R. Duan. Parametric eigenstructure assignment via output feedback based on singular value decompositions. *IEE Proceedings - Control Theory and Applications*, 150(1):93–100, 2003. doi: 10.1049/ip-cta:20030142.

[69] G. Ducard. *Fault-tolerant flight control and guidance systems: practical methods for small unmanned aerial vehicles.* Advances in industrial control. Springer, 2009. ISBN 9781848825604.

[70] G. Ducard and H. P. Geering. Efficient nonlinear actuator fault detection and isolation system for unmanned aerial vehicles. *Journal of Guidance, Control, and Dynamics*, 31(1): 225–237, 2008.

[71] W.C. Durham. Constrained control allocation. *Journal of Guidance, Control and Dynamics*, 16(4):717–725, 1993.

[72] W.C. Durham and K.A. Bordignon. Multiple control effector rate limiting. *Journal of guidance, control, and dynamics*, 19(1):30–37, 1996.

[73] A. Edelmayer. *Fault Detection in Dynamic Systems: From State Estimation to Direct Input Reconstruction.* Széchenyi University Press, Győr, 2012. ISBN 978-963-9819-88-7.

[74] A. Edelmayer, J. Bokor, F. Szigeti, and L. Keviczky. Robust detection filter design in the presence of time-varying system perturbations. *Automatica*, 33(3):471 – 475, 1997. doi: 10.1016/S0005-1098(96)00189-6.

[75] A. Edelmayer, J. Bokor, Z. Szabo, and F. Szigeti. Input reconstruction by means of system inversion: a geometric approach to fault detection and isolation in nonlinear systems. *International Journal of Applied Mathematics and Computer Science*, 14(2):189–200, 2004.

[76] C. Edwards and S.K. Spurgeon. *Sliding mode control: theory and applications.* Taylor & Francis systems and control book series. Taylor & Francis, 1998. ISBN 9780748406012.

[77] C. Edwards, S.K. Spurgeon, and R.J. Patton. Sliding mode observers for fault detection and isolation. *Automatica*, 36(4):541–553, 2000. doi: 10.1016/S0005-1098(99)00177-6.

[78] C. Edwards, T. Lombaerts, and H. Smaili. *Fault Tolerant Flight Control: A Benchmark Challenge.* Lecture Notes in Control and Information Sciences. Springer Verlag, 2010. ISBN 9783642116896.

[79] D. Efimov, J. Cieslak, and D. Henry. Supervisory fault tolerant control based on dwell-time conditions. In *18th IFAC World Congress, Milan, Italy*, volume 18, pages 13717–13722, 2011.

[80] D. Efimov, J. Cieslak, and D. Henry. Supervisory fault tolerant control with mutual performance optimization. *International Journal of Adaptive Control and Signal Processing*, 27(4):251–279, 2013. doi: 10.1002/acs.2296.

[81] A. Emami-Naeini, M. M. Akhter, and S. M. Rock. Effect of model uncertainty on failure detection: the threshold selector. *IEEE Transactions on Automatic Control*, 33(12):1106–1115, 1988. doi: 10.1109/9.14432.

[82] ESA. Mars Sample Return, 2014. URL `http://exploration.esa.int/jump.cfm?oid=44995`. Available online: 14-Aug-2014.

[83] L. Strippoli et. al. Integrated vision-based GNC for autonomous rendezvous and capture around mars. In *9th International ESA Conference on GNC Systems*, Porto, Portugal, 2014.

[84] J. S. Eterno, J. L. Weiss, D. P. Looze, and A. Wilsky. Design issues for fault tolerant-restructurable aircraft control. In *Proceedings of the 24th Conference on Decision and Control*, volume 2, pages 900–905, 1985.

[85] A. Falcoz, D. Henry, and A. Zolghadri. A nonlinear fault identification scheme for reusable launch vehicles control surfaces. *International Review of Aerospace Engineering*, 1(5):447–457, 2008.

[86] A. Falcoz, D. Henry, A. Zolghadri, E. Bornschleg, and M. Ganet. On-board model-based robust fdir strategy for reusable launch vehicles (rlv). In *7th International ESA Conference on GNC Systems*, Tralee, Ireland, 2008.

[87] A. Falcoz, F. Boquet, M. Dinh, B. Polle, G. Flandin, and E. Bornschlegl. Robust fault diagnosis strategies for spacecraft application to LISA pathfinder experiment. In *Automatic Control in Aerospace*, volume 18, pages 404–409, 2010.

[88] A. Falcoz, D. Henry, and A. Zolghadri. Robust fault diagnosis for atmospheric reentry vehicles: a case study. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 40(5):886–899, 2010. doi: 10.1109/TSMCA.2010.2063022.

[89] W. Fehse. *Automated rendezvous and docking of spacecraft*, volume 16. Cambridge university press, 2005.

[90] R. Fonod, D. Henry, E. Bornschlegl, and C. Charbonnel. Robust fault detection for systems with electronic induced delays: Application to the rendezvous phase of the MSR mission. In *Proceedings of the 12th European Control Conference*, pages 1439–1444, Zürich, Switzerland, July 2013.

[91] R. Fonod, D. Henry, C. Charbonnel, and E. Bornschlegl. A class of nonlinear unknown input observer for fault diagnosis: Application to fault tolerant control of an autonomous spacecraft. In *Proceedings of the 10th UKACC International Conference on Control*, Loughborough, United Kingdom, July 2014. IEEE.

[92] P. M. Frank. Advanced fault detection and isolation schemes using nonlinear and robust observers. In *Proc. of the 10th IFAC World Congress*, volume 3, pages 63–68, Munich, 1987.

[93] P. M. Frank. Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy - a survey and some new results. *Automatica*, 26:459–474, May 1990. doi: 10.1016/0005-1098(90)90018-D.

[94] P. M. Frank and J. Wünnenberg. Robust fault diagnosis using unknown input schemes. In R. J. Patton, P. M. Frank, and R. N. Clark, editors, *Fault Diagnosis in Dynamic Systems: Theory and Application*, chapter 3, pages 47–98. Prentice Hall, 1989.

[95] P.M. Frank and X. Ding. Frequency domain approach to optimally robust residual generation and evaluation for model-based fault diagnosis. *Automatica*, 30(5):789–804, 1994. doi: 10.1016/0005-1098(94)90169-4.

[96] P.M. Frank and X. Ding. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of Process Control*, 7(6):403 – 424, 1997. ISSN 0959-1524. doi: 10.1016/S0959-1524(97)00016-4.

[97] P.M. Frank, E.A. Garcia, and B. Köppen-Seliger. Modelling for fault detection and isolation versus modelling for control. *Mathematical and Computer Modelling of Dynamical Systems*, 7(1):1–46, 2001. doi: 10.1076/mcmd.7.1.1.3633.

[98] Gene F. Franklin, Michael L. Workman, and Dave Powell. *Digital Control of Dynamic Systems*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 3rd edition, 1997. ISBN 0201820544.

[99] Y. P. Fu, Y. H. Cheng, B. Jiang, and M. K. Yang. Fault tolerant control with on-line control allocation for flexible satellite attitude control system. In *2nd International Conference on Intelligent Control and Information Processing*, pages 42–46. IEEE, July 2011. doi: 10.1109/ICICIP.2011.6008195.

[100] P. Gahinet and P. Apkarian. A linear matrix inequality approach to H-infinity control. *International Journal of Robust and Nonlinear Control*, 4(4):421–448, 1994. ISSN 1099-1239.

[101] Z. Gao and P. Antsaklis. Stability of the pseudo-inverse method for reconfigurable control systems. *International Journal of Control*, 53(3):717–729, 1991.

[102] Z. Gao and J.A. Panos. Reconfigurable control system design via perfect model following. *International Journal of Control*, 56(4):783–798, 1992.

[103] E. Alcorta Garcia and P.M. Frank. Deterministic nonlinear observer-based approaches to fault diagnosis: A survey. *Control Engineering Practice*, 5(5):663–670, 1997. ISSN 0967-0661. doi: 10.1016/S0967-0661(97)00048-8.

[104] A. L. Gehin, M. Assas, and M. Staroswiecki. Structural analysis of system reconfigurability. In *In Proc. of IFAC Safeprocess*, volume 1, pages 292–297, 2000.

[105] J. Gertler. Fault detection and isolation using parity relations. *Control Engineering Practice*, 5(5):653–661, 1997. doi: 10.1016/S0967-0661(97)00047-6.

[106] J. Gertler. *Fault detection and diagnosis in engineering systems*. Marcel Dekker, 1998. ISBN 9780824794279.

[107] J. Gertler and M. Kunwer. Optimal residual decoupling for structured diagnosis and disturbance insensitivity. *International Journal of Control*, 61:395–421, 1995.

[108] E Gilbert and I. Kolmanovsky. Nonlinear tracking control in the presence of state and control constraints: a generalized reference governor. *Automatica*, 38(12):2063–2073, 2002. doi: 10.1016/S0005-1098(02)00135-8.

[109] Godard. *Fault Tolerant Control of Spacecraft*. PhD thesis, Ryerson University, Toronto, 2010.

[110] M. Gollor, M. Boss, F. de la Cruz, P. Galantini, and E. Bourguignon. Electric propulsion electronics activities in europe. In *Joint Propulsion Conferences*. AIAA, 2011. doi: 10.2514/6.2011-5517.

[111] G.H. Golub and C.F. Van Loan. *Matrix computations*, volume 3. Johns Hopkins University Press, 1996.

[112] W.S. Gosset. The probable error of a mean. *Biometrika*, pages 1–25, 1908.

[113] S. Grenaille, D. Henry, and A. Zolghadri. A method for designing fault diagnosis filters for lpv polytopic systems. *Journal of Control Science and Engineering*, 2008:1, 2008.

[114] J.E. Groszkiewicz and M. Bodson. Flight control reconfiguration using adaptive methods. In *34th IEEE Conference on Decision and Control*, volume 2, pages 1159–1164, dec 1995.

[115] P. Gurfil and N. J. Kasdin. Nonlinear modelling of spacecraft relative motion in the configuration space. *Journal of Guidance, Control, and Dynamics*, 27(1):154–157, 2004. doi: 10.2514/1.9343.

[116] F. Gustafsson. *Adaptive filtering and change detection*. Wiley Online Library, 2nd edition, 2001.

[117] H. Hammouri, M. Kinnaert, and E.H. El Yaagoubi. Observer-based approach to fault detection and isolation for nonlinear systems. *IEEE Transactions on Automatic Control*, 44(10):1879 –1884, oct 1999. ISSN 0018-9286. doi: 10.1109/9.793728.

[118] S. Hansen and M. Blanke. Diagnosis of airspeed measurement faults for unmanned aerial vehicles. *IEEE Transactions on Aerospace and Electronic Systems*, 50(1):224–239, 2014. doi: 10.1109/TAES.2013.120420.

[119] O. Härkegård and T. Glad. Resolving actuator redundancy - optimal control vs. control allocation. *Automatica*, 41(1):137 – 144, 2005. ISSN 0005-1098. doi: 10.1016/j.automatica.2004.09.007.

[120] O. Härkegård. *Backstepping and Control Allocation with Applications to Flight Control*. Linköping studies in science and technology. thesis no 820, Linköping University, Linköping, Sweden, May 2003.

[121] O. Härkegård. Dynamic control allocation using constrained quadratic programming. *Journal of Guidance Control and Dynamics*, 27(6):1028–1034, 2004.

[122] Ola Härkegård. Efficient active set algorithms for solving constrained least squares problems in aircraft control allocation. In *Proc. of Conference on Decision and Control*, pages 1295–1300, Las Vegas, NV, 2002.

[123] E. N. Hartley, P. A. Trodden, A. G. Richards, and J. M. Maciejowski. Model predictive control system design and implementation for spacecraft rendezvous. *Control Engineering Practice*, 20(7):695–713, 2012. ISSN 0967-0661. doi: 10.1016/j.conengprac.2012.03.009.

[124] S.S. Haykin et al. *Kalman filtering and neural networks*. Wiley Online Library, 2001.

[125] D. Henry. *Diagnostic et contrôle de cohérence des systèmes multivariables incertains*. PhD thesis, Université Bordeaux 1, France, 1999.

[126] D. Henry. Fault diagnosis of microscope satellite thrusters using H_∞/H_- filters. *Journal of Guidance, Control, and Dynamics*, 31(3):699–711, 2008. doi: 10.1109/TSMCA.2010.2063022.

[127] D. Henry. From fault diagnosis to recovery actions for aeronautic and aerospace missions: A model-based point of view. In *Proceedings of 23rd IAR Workshop on Advanced Control and Diagnosis*, pages 13–19, Coventry, UK, 2008.

[128] D. Henry. A norm-based point of view for fault diagnosis: Application to aerospace missions. *Automatic Control in Aerospace*, 4(1), march 2011.

[129] D. Henry. Structured fault detection filters for lpv systems modeled in an lfr manner. *International Journal of Adaptive Control and Signal Processing*, 26(3):190–207, 2012. doi: 10.1002/acs.1258.

[130] D. Henry. Design of norm based fault detection and isolation LPV filters. In *Robust Control and Linear Parameter Varying Approaches*, pages 125–180. Springer, 2013.

[131] D. Henry and A. Zolghadri. $H_\infty/H-$ filters for fault diagnosis in systems under feedback control. In *Proceedings of IFAC Safeprocess*, pages 87–92, Washington DC, USA, 2003.

[132] D. Henry and A. Zolghadri. Design and analysis of robust residual generators for systems under feedback control. *Automatica*, 41(2):251–264, 2005. doi: 10.1016/j.automatica.2004.09.013.

[133] D. Henry, A. Zolghadri, F. Castang, and M. Monsion. A new multi-objective filter design for guaranteed robust FDI performance. In *40th IEEE Conference on Decision and Control*, volume 1, pages 173–178, 2001.

[134] D. Henry, A. Zolghadri, F. Castang, and M. Monsion. A multi-objective filtering approach for fault diagnosis with guaranteed sensitivity performances. In *Proceedings of the 15th IFAC World Congress*, 2002.

[135] D. Henry, S. Simani, and R. Patton. Fault detection and diagnosis for aeronautic and aerospace missions. In C. Edwards, T. Lombaerts, and H. Smaili, editors, *Fault Tolerant Flight Control*, volume 399 of *Lecture Notes in Control and Information Sciences*, pages 91–128. Springer Verlag, 2010. doi: 10/fgx2wx.

[136] D. Henry, X. Olive, and E. Bornschlegl. A model-based solution for fault diagnosis of thruster faults: Application to the rendezvous phase of the Mars Sample Return mission. In *Proceeding of the 4th European Conference for Aerospace Sciences (EUCASS)*, St. Petersburg, Russian Federation, July 2011.

[137] D. Henry, J. Cieslak, A. Zolghadri, and D. Efimov. $H_\infty/H-$ LPV solutions for fault detection of aircraft actuator faults: Bridging the gap between theory and practice. *International Journal of Robust and Nonlinear Control*, page To appear, 2014. doi: 10.1002/rnc.3157.

[138] F.J.J. Hermans and M.B. Zarrop. Sliding mode observers for robust sensor monitoring. In *Proceedings of the 13th IFAC World Congress*, pages 211–216, 1996.

[139] L. Hetel, J. Daafouz, and C. Iung. Stabilization of arbitrary switched linear systems with unknown time-varying delays. *IEEE Transactions on Automatic Control*, 51(10): 1668–1674, 2006. doi: 10.1109/TAC.2006.883030.

[140] G. W. Hill. Researches in the lunar theory. *American Journal of Mathematics*, 1:5–26,129–147, and 245–260, 1878. ISSN 00029327.

[141] D. T. Horak. Experimental identification of modeling errors in dynamic systems. In *American Control Conference, 1988*, pages 1307 –1312, june 1988.

[142] M. Hou and P.C. Müller. Design of observers for linear systems with unknown inputs. *IEEE Transactions on Automatic Control*, 37(6):871–875, 1992. doi: 10.1109/9.256351.

[143] I. Hwang, S. Kim, Y. Kim, and C. E. Seah. A survey of fault detection, isolation, and reconfiguration methods. *IEEE Transactions on Control Systems Technology*, 18(3):636 –653, may 2010. ISSN 1063-6536. doi: 10.1109/TCST.2009.2026285.

[144] R. Isermann. Process fault detection based on modeling and estimation methods - a survey. *Automatica*, 20(4):387–404, 1984. doi: 10.1016/0005-1098(84)90098-0.

[145] R. Isermann. Model-based fault-detection and diagnosis - status and applications. *Annual Reviews in Control*, 29(1):71 – 85, 2005. doi: 10.1016/j.arcontrol.2004.12.002.

[146] R. Isermann. *Fault Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Springer Verlag, Berlin, 2006. ISBN 9783540241126.

[147] R. Isermann and P. Ballé. Trends in the application of model-based fault detection and diagnosis of technical processes. *Control Engineering Practice*, 5(5):709 – 719, 1997. ISSN 0967-0661. doi: 10.1016/S0967-0661(97)00053-1.

[148] R. Isermann, R. Schwarz, and S. Stolzl. Fault-tolerant drive-by-wire systems. *Control Systems, IEEE*, 22(5):64 – 81, oct 2002. ISSN 1066-033X. doi: 10.1109/MCS.2002.1035218.

[149] A. Isidori. *Nonlinear control systems, 2nd edition*. Springer-Verlag, 1989.

[150] B. Jiang, M. Staroswiecki, and V. Cocquempot. h_∞ fault detection filter design for linear discrete-time systems with multiple time delays. *International Journal of Systems Science*, 34(5):365–373, 2003. doi: 10.1080/00207720310001601037.

[151] B. Jiang, M. Staroswiecki, and V. Cocquempot. Fault accommodationfor nonlinear dynamic systems. *IEEE Transactions on Automatic Control*, 51(9):1578 –1583, sept. 2006. ISSN 0018-9286. doi: 10.1109/TAC.2006.878732.

[152] C. Jiang and D. H. Zhou. Fault detection and identification for uncertain linear time-delay systems. *Computers & chemical engineering*, 30(2):228–242, 2005. doi: 10.1016/j.compchemeng.2005.08.012.

[153] J. Jiang. Design of reconfigurable control systems using eigenstructure assignments. *International Journal of Control*, 59(2):395–410, 1994.

[154] Y. Jiang, Q. Hu, and G. Ma. Adaptive backstepping fault-tolerant control for flexible spacecraft with unknown bounded disturbances and actuator failures. *ISA transactions*, 49(1):57–69, 2010.

[155] H. P. Jin, P. Wiktor, and D. B. DeBra. An optimal thruster configuration design and evaluation for quick step. *Control Engineering Practice*, 3(8):1113–1118, 1995. doi: 10.1016/0967-0661(95)00104-3.

[156] J. Jin, B. Park, Y. Park, and M-J Tahk. Attitude control of a satellite with redundant thrusters. *Aerospace Science and Technology*, 10:644–651, 2006. doi: 10.1016/j.ast.2006.04.005.

[157] T. A. Johansen and T. I. Fossen. Control allocation - A survey. *Automatica*, 49(5): 1087–1103, 2013. doi: 10.1016/j.automatica.2013.01.035.

[158] S.J. Julier and J.K. Uhlmann. A new extension of the kalman filter to nonlinear systems. In *Int. Symp. Aerospace/Defense Sensing, Simul. and Controls*, volume 3, page 26. Spie Bellingham, WA, 1997.

[159] S. Kanev and M. Verhaegen. Controller reconfiguration for non-linear systems. *Control Engineering Practice*, 8(11):1223–1236, 2000. doi: 10.1016/S0967-0661(00)00074-5.

[160] H. R. Karimi, M. Zapateiro, and N. Luo. A linear matrix inequality approach to robust fault detection filter design of linear systems with mixed time-varying delays and nonlinear perturbations. *Journal of the Franklin Institute*, 347(6):957–973, 2010. doi: 10.1016/j.jfranklin.2010.03.004.

[161] E.C. Kerrigan and J.M. Maciejowski. Invariant sets for constrained nonlinear discrete-time systems withapplication to feasibility in model predictive control. In *Proceedings of the IEEE Conference on Decision and Control*, volume 5, pages 4951–4956, 2000.

[162] A. Khelassi, P. Weber, and D. Theilliol. Reconfigurable control design for over-actuated systems based on reliability indicators. In *Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 365–370. IEEE, 2010.

[163] K.S. Kim, K.J. Lee, and Y. Kim. Reconfigurable flight control system design using direct adaptive method. *Journal of guidance, control, and dynamics*, 26(4):543–550, 2003. doi: 10.2514/2.5103.

[164] I. Konstantopoulos and P. Antsaklis. An eigenstructure assignment approach to control reconfiguration. In *Proceedings of the 4th IEEE Mediterranean Symposium on Control et Automation, Chania, Crete, Greece*, pages 328–333, 1996.

[165] J. Korbicz, J.M. Koscielny, and Z. Kowalczuk. *Fault diagnosis: models, artificial intelligence, applications*. Engineering online library. Springer, 2004. ISBN 9783540407676.

[166] F Kratz, W Nuninger, and S Ploix. Fault detection for time-delay systems: a parity space approach. In *American Control Conference*, volume 4, pages 2009–2011, Philadelphia, USA, 1998. IEEE. doi: 10.1109/ACC.1998.702978.

[167] D. Krokavec and A. Filasová. *Optimal Stochastic Systems (in Slovak)*. Elfa, Košice, Slovak Republic, 2002.

[168] D. Krokavec and A. Filasová. *Dynamic Systems Diagnosis (in Slovak)*. Elfa, Košice, Slovak Republic, 2007.

[169] D. Krokavec and A. Filasová. *Discrete-Time Systems (in Slovak)*. Elfa, Košice, Slovak Republic, 2008.

[170] W. Kutta. Beitrag zur näherungsweisen integration totaler differentialgleichungen. *Zeitschrift für Mathematik und Physik*, 46:435–453, 1901.

[171] M. Kvasnica, J. Löfberg, and M. Fikar. Stabilizing polynomial approximation of explicit mpc. *Automatica*, 47(10):2292–2297, 2011. doi: 10.1016/j.automatica.2011.08.023.

[172] W. J. Lee, L. A. D'Amario, R. B. Roncoli, and J. C. Smith. Mission Design Overview for Mars 2003/2005 Sample Return Mission. In *AIAA/AAS Astrodynamics Specialist Conference*, Girdwood, USA, August 1999.

[173] E. J. Lefferts, F. L. Markley, and M. D. Shuster. Kalman filtering for spacecraft attitude estimation. *Journal of Guidance, Control, and Dynamics*, 5(5):417–429, 1982. doi: 10.2514/6.1982-70.

[174] IE Leonard. The matrix exponential. *SIAM review*, 38(3):507–512, 1996. doi: 10.1137/S0036144595286488.

[175] F.L. Lewis and FL Lewis. *Optimal estimation: with an introduction to stochastic control theory*. Wiley New York, 1986.

[176] F. Liao, J. L. Wang, and G. H. Yang. Reliable robust flight tracking control: an lmi approach. *IEEE Transactions on Control Systems Technology*, 10(1):76 –89, jan 2002. ISSN 1063-6536. doi: 10.1109/87.974340.

[177] G.P. Liu and R.J. Patton. *Eigenstructure assignment for control system design*. John Wiley & Sons, Inc., 1998.

[178] J.S. Liu and R. Chen. Sequential monte carlo methods for dynamic systems. *Journal of the American statistical association*, pages 1032–1044, 1998.

[179] D. Looze, J. Weiss, J. Eterno, and N. Barrett. An automatic redesign approach for restructurable control systems. *IEEE Control Systems Magazine*, 5(2):16 –22, may 1985. ISSN 0272-1708.

[180] Per Lötstedt. Solving the minimal least squares problem subject to bounds on the variables. *BIT Numerical Mathematics*, 24(2):205–224, 1984.

[181] X. C. Lou, A. S. Willsky, and G. C. Verghese. Optimally robust redundancy relations for failure detection in uncertain systems. *Automatica*, 22(3):333–344, 1986. doi: 10.1016/0005-1098(86)90031-2.

[182] D. Luenberger. Observers for multivariable systems. *IEEE Transactions on Automatic Control*, 11(2):190 – 197, apr 1966. doi: 10.1109/TAC.1966.1098323.

[183] J. Lunze and J. Richter. Control reconfiguration: Survey of methods and open problems. Technical report, Ruhr-Universität Bochum, Lehrstuhl für Automatisierungstechnik und Prozessinformatik, 2006.

[184] J.M Maciejowski. Reconfigurable control using constrained optimization. In *Proceeding of European Control Conference ECC97, Brussels, Belgium*, pages 107–130. Citeseer, 1997.

[185] J.M. Maciejowski and C.N. Jones. MPC fault-tolerant flight control case study: Flight 1862. In *Proceedings of the 5th IFAC Safeprocess Conference*, 2003.

[186] R. S. Mangoubi. *Robust estimation and failure detection: A concise treatment*. Springer Verlag, 1998.

[187] R. S. Mangoubi and A. Edelmayer. Model-based fault detection: the optimal past, the robust present and a few thoughts on the future. In *Proceedings of the 4th IFAC Safeprocess*, pages 64–75, Budapest, Hungary, 2000.

[188] A. Marcos and G. Balas. A robust integrated controller/diagnosis aircraft application. *International Journal of Robust and Nonlinear Control*, 15(12):531–551, 2005.

[189] A. Marcos and L. F. Penin. Deimos experience, insight and perspective on space FDIR. In *5th ESA Workshop on Avionics Data, Control and Software Systems*, Noordwijk, The Netherlands, 2011.

[190] M.A. Massoumnia. A geometric approach to the synthesis of failure detection filters. *IEEE Transactions on Automatic Control*, 31(9):839–846, sep 1986. ISSN 0018-9286. doi: 10.1109/TAC.1986.1104419.

[191] P. S. Maybeck. Multiple model adaptive algorithms for detecting and compensating sensor and actuator/surface failures in aircraft flight control systems. *International Journal of Robust and Nonlinear Control*, 9(14):1051–1070, 1999.

[192] P. S. Maybeck and D. L. Pogoda. Multiple model adaptive controller for the stol f-15 with sensor/actuator failures. In *Proceedings of the 28th IEEE Conference on Decision and Control*, pages 1566–1572. IEEE, 1989.

[193] A. Medvedev. Fault detection and isolation by a continuous parity space method. *Automatica*, 31(7):1039 – 1044, 1995. ISSN 0005-1098. doi: 10.1016/0005-1098(95)00008-K.

[194] N. Meskin and K. Khorasani. Robust fault detection and isolation of time-delay systems using a geometric approach. *Automatica*, 45(6):1567–1573, 2009. doi: 10.1016/j.automatica.2009.02.019.

[195] Y.V. Mikheev, VA Sobolev, and E. Fridman. Asymptotic analysis of digital control systems. *Automation and Remote Control*, 49(9):1175–1180, 1988.

[196] K. S. Miller. On the inverse of the sum of matrices. *Mathematics Magazine*, pages 67–72, 1981.

[197] O. Montenbruck and E. Gill. *Satellite orbits*. Springer, 2000.

[198] M. Morari, M. Baotic, and F. Borrelli. Hybrid systems modeling and control. *European Journal of Control*, 9(2-3):177–189, 2003.

[199] J.C. Morris, California Institute of Technology. Division of Engineering, and Applied Science. *Experimental Control and Model Validation: A Helicopter Case Study*. CIT theses. California Institute of Technology, 1996.

[200] K. E. Murphy. Light detection and ranging (lidar) mapping system, March 2004. US Patent No. 6 ,711, 475.

[201] I. Nagesh and C. Edwards. A sliding mode observer based fdi scheme for a nonlinear satellite systems. In *IEEE International Conference on Control Applications (CCA)*, pages 159 –164, sept. 2011.

[202] I. Nagesh and C. Edwards. A sliding mode observer based sensor fault detection and isolation scheme for a nonlinear satellite system. In *12th International Workshop on Variable Structure Systems (VSS)*, pages 248 –253, jan. 2012.

[203] K.S. Narendra and J. Balakrishnan. Adaptive control using multiple models. *IEEE Transactions on Automatic Control*, 42(2):171–187, 1997. doi: 10.1109/9.554398.

[204] J Neyman and ES Pearson. On the problem of the most efficient tests of statistical hypotheses. *Royal Society of London Philosophical Transactions Series A*, 231:289–337, 1933.

[205] H. Niemann and J. Stoustrup. Multi objective design techniques applied to fault detection and isolation. In *Proceedings of the American Control Conference*, volume 4, pages 2022–2026. IEEE, 1998.

[206] H. Niemann and J. Stoustrup. Gain scheduling using the youla parametrization. In *Proceedings of Conference on Decision and Control*, New York, USA, 1999. IEEE.

[207] H. Niemann and J. Stoustrup. Passive fault tolerant control of a double inverted pendulum - a case study. *Control Engineering Practice*, 13(8):1047 – 1059, 2005. ISSN 0967-0661. doi: 10.1016/j.conengprac.2004.11.002.

[208] M. Nørgaard, N.K. Poulsen, and O. Ravn. New developments in state estimation for nonlinear systems. *Automatica*, 36(11):1627–1638, 2000. doi: 10.1016/S0005-1098(00)00089-3.

[209] H. Noura, D. Sauter, and F. Hamelin. Evaluation of a fault-tolerant control design for actuator faults. In *Proceedings of the 36th IEEE Conference on Decision and Control*, volume 4, pages 3982–3983. IEEE, 1997.

[210] H. Noura, D. Theilliol, J.C. Ponsart, and A. Chamseddine. *Fault-tolerant Control Systems: Design and Practical Applications*. Advances in Industrial Control. Springer Verlag, London, 2009. ISBN 9781848826526.

[211] M. Nyberg. A generalization of the gde minimal hitting-set algorithm to handle behavioral modes. In *Proceedings of the 14th International Workshop on Principles of Diagnosis, DX*, 2006.

[212] M. Nyberg. A fault isolation algorithm for the case of multiple faults and multiple fault types. *Proceedings of IFAC Safeprocess*, 2006.

[213] Statement of Work. *Integrated GNC Solutions for Autonomous Mars Rendezvous and Capture*. SRE_PAP/MREP/GNCRVC-SOW. Issue 2, Revision 5. 27th August, 2010.

[214] X. Olive. FDI(R) for satellites: How to deal with high availability and robustness in the space domain? *International Journal of Applied Mathematics and Computer Science*, 22 (1):99–107, 2012. doi: 10.2478/v10006-012-0007-8.

[215] E. Omerdic. *Thruster Fault-Tolerant Control: Thruster Fault Diagnosis and Accommodation System ForUnderwater Vehicles*. VDM Publishing, 2009. ISBN 9783639117394.

[216] M. Oppenheimer, D. Doman, and M. Bolender. Control allocation. In W. S. Levine, editor, *The control handbook, control system applications (2nd ed., Chapter 8)*. CRC Press, 2010.

[217] S. Osder. Practical view of redundancy management application and theory. *Journal of Guidance, Control, and Dynamics*, 22(1):12–21, 1999. doi: 10.2514/2.4363.

[218] Aaron J. Ostroff. Techniques for accommodating control effector failures on a mildly statically unstable airplane. In *American Control Conference*, pages 906 –913, june 1985.

[219] A.B. Page and M.L. Steinberg. High-fidelity simulation testing of control allocation methods. In *AIAA Guidance, Navigation and Control Conference and Exhibit*, Monterey, California, 2002. AIAA. doi: 10.2514/6.2002-4547.

[220] E.S. Page. Continuous inspection schemes. *Biometrika*, pages 100–115, 1954.

[221] A. Papoulis and R.V. Probability. *Stochastic processes*, volume 3. McGraw-Hill, New York, 1991.

[222] R. J Patton and J. Chen. Robust fault detection of jet engine sensor systems using eigenstructure assignment. *Journal of Guidance, Control, and Dynamics*, 15(6):1491–1497, 1992. doi: 10.2514/3.11413.

[223] R.J. Patton. Robustness in model-based fault diagnosis: The 1995 situation. *Annual Reviews in Control*, 21(0):103 – 123, 1997. ISSN 1367-5788. doi: 10.1016/S1367-5788(97)00020-5.

[224] R.J. Patton. Fault-tolerant control systems: The 1997 situation. In *Proceedings of the IFAC Safeprocess*, volume 3, pages 1033–1054, Kingston Upon Hull, United Kingdom, 1997.

[225] R.J. Patton and J. Chen. Robust fault detection using eigenstructure assignment: A tutorial consideration and some new results. In *Proceedings of the 30th IEEE Conference on Decision and Control*, pages 2242–2247. IEEE, 1991.

[226] R.J. Patton and J. Chen. Optimal unknown input distribution matrix selection in robust fault diagnosis. *Automatica*, 29(4):837–841, 1993. doi: 10.1016/0005-1098(93)90089-C.

[227] R.J. Patton and J. Chen. Review of parity space approaches to fault diagnosis for aerospace systems. *Journal of Guidance Control Dynamics*, 17:278–285, 1994.

[228] R.J. Patton and J. Chen. Observer-based fault detection and isolation: robustness and applications. *Control Engineering Practice*, 5(5):671–682, 1997. doi: 10.1016/S0967-0661(97)00049-X.

[229] R.J. Patton and P. M. Frank. *Fault Diagnosis in Dynamic Systems: Theory and Application.* Prentice Hall, 1989.

[230] RJ Patton, SW Willcox, and JS Winter. Parameter-insensitive technique for aircraft sensor fault analysis. *Journal of Guidance, Control, and Dynamics*, 10(4):359–367, 1987. doi: 10.2514/3.20226.

[231] R.J. Patton, P. Frank, and R.N. Clark. *Issues of fault diagnosis for dynamic systems.* Springer, London, 2000.

[232] R.J. Patton, F.J. Uppal, S. Simani, and B. Polle. Reliable fault diagnosis scheme for a spacecraft attitude control system. *Journal of Risk and Reliability*, 222:139–152, 2008. doi: 10.1243/1748006XJRR98.

[233] R.J. Patton, F.J. Uppal, S. Simani, and B. Polle. Reliable fault diagnosis scheme for a spacecraft attitude control system. *Proceedings of the Institution of Mechanical Engineers Part O: Journal of Risk and Reliability*, 222:139–152, 2008. doi: 10.1243/1748006XJRR98.

[234] R.J. Patton, F.J. Uppal, S. Simani, and B. Polle. Robust fdi applied to thruster faults of a satellite system. *Control Engineering Practice*, 18(9):1093–1109, 2010. doi: 10.1016/j.conengprac.2009.04.011.

[235] F. Pelletier, D. Golla, and A. Allen. Lidar-based rendezvous navigation for MSR. In *Guidance, Navigation, and Control and Co-located Conferences.* AIAA, Providence, Rhode Island, 2004. doi: 10.2514/6.2004-4987.

[236] J. A. M. Petersen and M. Bodson. Constrained quadratic programming techniques for control allocation. *IEEE Transactions on Control Systems Technology*, 14(1):91–98, 2006. doi: 10.1109/TCST.2005.860516.

[237] L. Pettazzi, A. Lanzon, S. Theil, and A.E. Finzi. Design of robust drag-free controllers with given structure. *Journal of Guidance, Control, and Dynamics*, 32(5):1609–1621, 2009. doi: 10.2514/1.40279.

[238] C. L. Peuvédic, M. Massimiliano, J. de Lafontaine, A. Kron, and G. Ortega. Key control techniques for gnc design of martian vehicles. In *6th International ESA Conference on GNC Systems*, Loutraki, Greece, 2005.

[239] C. L. Peuvédic, P. Colmenarejo, and A. Guiotto. Autonomous Rendezvous Control System: a High Fidelity Functional Engineering Simulator Developed for GNC/AMM/FDIR Validation. In *7th International ESA Conference on GNC Systems*, Tralee, Ireland, 2008.

[240] C. L. Peuvédic, C. Charbonnel, D. Henry, L. Strippoli, and F. Ankersen. Fault tolerant control design for terminal rendezvous around mars. In *9th International ESA Conference on GNC Systems*, page June, Portugal, 2014.

[241] J.D. Pintér. *Global optimization in action: continuous and Lipschitz optimization–algorithms, implementations, and applications*, volume 6. Springer, 1996.

[242] M.K. Pitt and N. Shephard. Filtering via simulation: Auxiliary particle filters. *Journal of the American Statistical Association*, pages 590–599, 1999.

[243] M.M. Polycarpou. Fault accommodation of a class of multivariable nonlinear dynamical systems using a learning approach. *IEEE Transactions on Automatic Control*, 46(5):736 –742, may 2001. ISSN 0018-9286. doi: 10.1109/9.920792.

[244] M.M. Polycarpou and A.J. Helmicki. Automated fault detection and accommodation: a learning systems approach. *IEEE Transactions on Systems, Man and Cybernetics*, 25(11): 1447 –1458, nov 1995. ISSN 0018-9472. doi: 10.1109/21.467710.

[245] C. M. Pong. *Autonomous thruster failure recovery for underactuated spacecraft*. PhD thesis, Massachusetts Institute of Technology, 2010.

[246] A. Posch, A.O. Schwientek, J. Sommer, and W. Fichter. Model-based on-board real-time thruster fault monitoring. In *Proceedings of IFAC Symposium on Automatic Control in Aerospace*, pages 553–558, Würzburg, Germany, 2013. doi: 10.3182/20130902-5-DE-2040.00080.

[247] F. Pukelsheim. The three sigma rule. *The American Statistician*, 48(2):88–91, 1994.

[248] S.J. Raza and J.T. Silverthorn. Use of pseudo inverse for design of a reconfigurable flight control system. In *AIAA Guidance, Navigation and Control Conference*, pages 349 – 356, 1985.

[249] R. Reiter. A theory of diagnosis from first principles. *Artificial intelligence*, 32(1):57–95, 1987. doi: 10.1016/0004-3702(87)90062-2.

[250] J.H. Richter. *Reconfigurable Control of Nonlinear Dynamical Systems: A Fault-Hiding Approach*. Lecture Notes in Control and Information Sciences. Springer, 2011. ISBN 9783642176272.

[251] Brent Robertson and Eric Stoneking. Satellite gn & c anomaly trends. *Advances in the Astronautical Sciences*, 113:531–542, 2003.

[252] B. Sadeghi and B. Moshiri. Second-order ekf and unscented kalman filter fusion for tracking maneuvering targets. In *IEEE International Conference on Information Reuse and Integration*, pages 514–519. IEEE, 2007.

[253] M. G. Safonov. Focusing on the knowable. In *Control using logic-based switching*, pages 224–233. Springer, 1997.

[254] M. G. Safonov and F. B. Cabral. Fitting controllers to data. *Systems & Control Letters*, 43(4):299–308, 2001.

[255] M. G. Safonov and T. C. Tsao. The unfalsified control concept and learning. *IEEE Transactions on Automatic Control*, 42(6):843–847, 1997. doi: 10.1109/9.587340.

[256] H. Schaub and J. L. Junkins. *Analytical Mechanics of Space Systems*. AIAA Education Series, Reston, VA, 2nd edition, 2009.

[257] R. Seliger and P. M. Frank. Robust component fault detection and isolation in nonlinear dynamic dynamic systems using unknown input observers. In *Proceedings of IFAC SAFEPROCESS*, pages 313–318, Baden-Baden, Germany, 1991. IFAC-IMACS.

[258] R. Seliger and P. M. Frank. Fault diagnosis by disturbance decoupled nonlinear observers. In *Proceedings of the 30th Conference on Decision and Control*, pages 2248–2253, Brighton, England, 1991.

[259] M. J. Sidi. *Spacecraft dynamics and control: a practical engineering approach*, volume 7. Cambridge university press, 1997.

[260] S. Simani, C. Fantuzzi, and R. Patton. *Model-based fault diagnosis in dynamic systems using identification techniques*. Springer New York, 2003.

[261] P. Singla, K. Subbarao, and J. L. Junkins. Adaptive output feedback control for spacecraft rendezvous and docking under measurement uncertainty. *Journal of Guidance, Control, and Dynamics*, 29(4):892–902, 2006. doi: 10.2514/1.17498.

[262] K.M. Sobel, E.Y. Shapiro, and AN Andry. Eigenstructure assignment. *International Journal of Control*, 59:13–13, 1994.

[263] M. Staroswiecki. On reconfigurability with respect to actuator failures. In *IFAC World Congress, Barcelona, Spain*, 2002.

[264] M. Staroswiecki. Progressive accommodation of actuator faults in the linear quadratic control problem. In *Decision and Control, 2004. CDC. 43rd IEEE Conference on*, volume 5, pages 5234 – 5241 Vol.5, dec. 2004.

[265] M. Staroswiecki. Fault tolerant control: the pseudo-inverse method revisited. In *16th IFAC World Congress*, 2005.

[266] M. Staroswiecki and D. Berdjag. A general fault tolerant linear quadratic control strategy under actuator outages. *International Journal of Systems Science*, 41(8):971–985, 2010.

[267] T. Steffen. *Control reconfiguration of dynamical systems: linear approaches and structural tests*. Lecture notes in control and information sciences. Springer Verlag, 2005. ISBN 9783540257301.

[268] M. Steinberg. Historical overview of research in reconfigurable flight control. *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, 219 (4):263–275, 2005.

[269] R. Stengel and C. Huang. Restructurable control using proportional-integral implicit model following((for fighter aircraft)). *Journal of Guidance, Control, and Dynamics*, 13: 303–309, 1990.

[270] J. Stoustrup and H. H Niemann. Fault estimation - a standard problem approach. *International Journal of Robust and Nonlinear Control*, 12(8):649–673, 2002.

[271] F. Szigeti, A. Rios-Bolivar, and R. Tarantino. Fault detection and isolation filter design by inversion: The case of linear systems. In A. Edelmayer, editor, *Proceedings of the 4th IFAC Safeprocess*, volume 2, pages 387–392, London, 2000. Pergamon Press.

[272] M. Tafazoli. A study of on-orbit spacecraft failures. *Acta Astronautica*, 64(2):195–205, 2009. doi: 10.1016/j.actaastro.2008.07.019.

[273] C.P. Tan and C. Edwards. Sliding mode observers for detection and reconstruction of sensor faults. *Automatica*, 38(10):1815–1821, 2002. doi: 10.1016/S0005-1098(02)00098-5.

[274] C.P. Tan and C. Edwards. Sliding mode observers for robust detection and reconstruction of actuator and sensor faults. *International Journal of Robust and Nonlinear Control*, 13 (5):443–463, 2003. doi: 10.1002/rnc.723.

[275] G. Tao, S. Chen, and S.M. Joshi. An adaptive actuator failure compensation controller using output feedback. *IEEE Transactions on Automatic Control*, 47(3):506 –511, mar 2002. ISSN 0018-9286. doi: 10.1109/9.989150.

[276] Y. Tharrault, G. Mourot, J. Ragot, and D. Maquin. Fault detection and isolation with robust principal component analysis. *International Journal of Applied Mathematics and Computer Science*, 18(4):429–442, 2008.

[277] D. Theilliol, D. Sauter, and J. C. Ponsart. A multiple model based approach for fault tolerant control in non linear systems. In *Proceedings of the 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Washington, DC, USA*, volume 1, pages 149–154, Washington, DC, USA, 2003.

[278] D. Theilliol, Y. M. Zhang, and J. C. Ponsart. Fault tolerant control system against actuator failures based on re-configuring reference input. In *International Conference on Advances in Computational Tools for Engineering Applications*, pages 480–485. IEEE, 2009.

[279] C. Tsui. A new dynamic output feedback compensator design for pole assignment. *Journal of the Franklin Institute*, 336(4):665–674, 1999.

[280] J. Jr. Tyler. The characteristics of model-following systems as synthesized by optimal control. *IEEE Transactions on Automatic Control*, 9(4):485 – 498, oct 1964. ISSN 0018-9286. doi: 10.1109/TAC.1964.1105757.

[281] V.I. Utkin. *Sliding modes in control and optimization*, volume 116. Springer Verlag, Berlin, 1992.

[282] A. Varga. New computational approach for the design of fault detection and isolation filters. In Mihail Voicu, editor, *Advances in Automatic Control*, volume 754 of *The Kluwer International Series in Engineering and Computer Science*, pages 367–381. Springer, 2003. ISBN 978-1-4419-9184-3. doi: 10/d9tr5s.

[283] R.J. Veillette, J.B. Medanic, and W.R. Perkins. Design of reliable control systems. *IEEE Transactions on Automatic Control*, 37(3):290 –304, mar 1992. ISSN 0018-9286. doi: 10.1109/9.119629.

[284] V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S.N. Kavuri. A review of process fault detection and diagnosis: Part i-iii. *Computers & Chemical Engineering*, 27(3):293–346, 2003.

[285] M. Verhaegen, S. Kanev, R. Hallouzi, C. Jones, J. Maciejowski, and H. Smail. Fault tolerant flight control - a survey. *Fault Tolerant Flight Control*, pages 47–89, 2010.

[286] J. C. Virnig and D. S. Bodden. Multivariable control allocation and control law conditioning when control effectors limit. In *AIAA Guidance, Navigation and Control Conference, Scottsdale, AZ*, pages 572–582, 1994.

[287] A. Wald. *Sequential Analysis*. Dover Publications, 1947.

[288] E.A. Wan and R. Van Der Merwe. The unscented kalman filter for nonlinear estimation. In *Adaptive Systems for Signal Processing, Communications, and Control Symposium 2000*, pages 153–158. IEEE, 2000.

[289] A. Wander and R. Förstner. Innovative fault detection, isolation and recovery strategies on-board spacecraft: State of the art and research challenges. In *Proc. of Deutscher Luft- und Raumfahrkongress*, Berlin, 2012.

[290] A.P. Wang and S.F. Lin. The parametric solutions of eigenstructure assignment for controllable and uncontrollable singular systems. *Journal of mathematical analysis and applications*, 248(2):549–571, 2000.

[291] H. Wang and S. Daley. Actuator fault diagnosis: an adaptive observer-based technique. *IEEE Transactions on Automatic Control*, 41(7):1073 –1078, jul 1996. ISSN 0018-9286. doi: 10.1109/9.508919.

[292] W. Wang and C. Wen. Adaptive actuator failure compensation control of uncertain nonlinear systems with guaranteed transient performance. *Automatica*, 46(12):2082–2091, 2010. doi: 10.1016/j.automatica.2010.09.006.

[293] W. Wang and C. Wen. Adaptive compensation for infinite number of actuator failures or faults. *Automatica*, 47(10):2197–2210, 2011. doi: 10.1016/j.automatica.2011.08.022.

[294] Y. Wang, S. X. Ding, H. Ye, and G. Wang. A new fault detection scheme for networked control systems subject to uncertain time-varying delay. *IEEE Transactions on Signal Processing*, 56(10):5258–5268, 2008. doi: 10.1109/TSP.2008.928703.

[295] J. R. Wertz. *Spacecraft attitude determination and control*, volume 73. D. Reidel Publishing Company, Boston, AM, 1978.

[296] B. Wie. *Space vehicle dynamics and control*. AIAA Education Series, Reston, VA, 1998.

[297] R. Wisniewski. Lecture notes on modeling of a spacecraft, 1999. URL `http://vbn.aau.dk/files/106321/fulltext`.

[298] W Murray Wonham. *Linear multivariable control*. Springer, 1974.

[299] W.M. Wonham and A.S. Morse. Decoupling and pole assignment in linear multivariable systems: a geometric approach. *SIAM J. Control*, 8(1):1–18, 1970.

[300] H. Yang and M. Saif. Observer design and fault diagnosis for state-retarded dynamical systems. *Automatica*, 34(2):217 – 227, 1998. doi: http://dx.doi.org/10.1016/S0005-1098(97)00175-1.

[301] H. Yang, B. Jiang, and V. Cocquempot. A fault tolerant control framework for periodic switched non-linear systems. *International Journal of Control*, 82(1):117–129, 2009.

[302] H. Yang, B. Jiang, and M. Staroswiecki. Supervisory fault tolerant control for a class of uncertain nonlinear systems. *Automatica*, 45(10):2319–2324, 2009. doi: 10.1016/j.automatica.2009.06.019.

[303] H. Yang, B. Jiang, and V. Cocquempot. *Fault tolerant control design for hybrid systems*, volume 397. Springer Verlag, 2010.

[304] R.K. Yedavalli. Stability robustness measures under dependent uncertainty. In *American Control Conference*, pages 820–823. IEEE, 1988.

[305] Peter Young. Parameter estimation for continuous-time models: A survey. *Automatica*, 17(1):23–39, 1981. doi: 10.1016/0005-1098(81)90082-0.

[306] Y. Zhan and J. Jiang. An interacting multiple-model based fault detection, diagnosis and fault-tolerant control approach. In *Proceedings of the 38th IEEE Conference on Decision and Control*, volume 4, pages 3593–3598. IEEE, 1999.

[307] F. Zhang, G. Liu, and L. Fang. Actuator fault estimation based on adaptive h_∞ observer technique. In *International Conference on Mechatronics and Automation*, pages 352 –357, aug. 2009. doi: 10.1109/ICMA.2009.5246667.

[308] X. Zhang, M.M. Polycarpou, and T. Parisini. A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems. *IEEE Transactions on Automatic Control*, 47(4):576–593, 2002. doi: 10.1109/9.995036.

[309] X. Zhang, M.M. Polycarpou, and T. Parisini. Fault diagnosis of a class of nonlinear uncertain systems with lipschitz nonlinearities using adaptive estimation. *Automatica*, 46 (2):290–299, 2010. doi: 10.1016/j.automatica.2009.11.014.

[310] Y. Zhang and J. Jiang. Integrated active fault-tolerant control using imm approach. *IEEE Transactions on Aerospace and Electronic Systems*, 37(4):1221–1235, 2001.

[311] Y. Zhang and J. Jiang. Fault tolerant control system design with explicit consideration of performance degradation. *IEEE Transactions on Aerospace and Electronic Systems*, 39 (3):838–848, 2003. doi: 10.1109/TAES.2003.1238740.

[312] Y. Zhang and J. Jiang. Bibliographical review on reconfigurable fault-tolerant control systems. *Annual Reviews in Control*, 32(2):229–252, 2008. doi: 10.1016/j.arcontrol.2008.03.008.

[313] Y. Zhang, V.S. Suresh, B. Jiang, and D. Theilliol. Reconfigurable control allocation against aircraft control effector failures. In *IEEE International Conference on Control Applications*, pages 1197–1202, 2007. doi: 10.1109/CCA.2007.4389398.

[314] Y. Zhenyu, S. Huazhang, and C. Zongji. The frequency-domain heterogeneous control mixer module method for control reconfiguration. In *IEEE International Conference on Control Applications*, volume 2, pages 1223–1228. IEEE, 1999.

[315] M. Zhong, S. X. Ding, J. Lam, and H. Wang. An LMI approach to design robust fault detection filter for uncertain LTI systems. *Automatica*, 39(3):543–550, 2003. doi: 10.1016/S0005-1098(02)00269-8.

[316] K. Zhou and P. Khargonekar. Stability robustness bounds for linear state-space models with structured uncertainty. *IEEE Transactions on Automatic Control*, 32(7):621–623, 1987. doi: 10.1109/TAC.1987.1104667.

[317] K. Zhou and P. P. Khargonekar. Robust stabilization of linear systems with norm-bounded time-varying uncertainty. *Systems & Control Letters*, 10(1):17–20, 1988.

[318] A. Zolghadri. An algorithm for real-time failure detection in kalman filters. *IEEE Transactions on Automatic Control*, 41(10):1537–1539, 1996. doi: 10.1109/9.539440.

[319] A. Zolghadri. The challenge of advanced model-based fdir techniques for aerospace systems: the 2011 situation. In *Proceeding of the 4th European Conference for Aerospace Sciences (EUCASS)*, St. Petersburg, Russian Federation, 2011.

[320] A. M. Zou and K. D. Kumar. Adaptive fuzzy fault-tolerant attitude control of spacecraft. *Control Engineering Practice*, 19(1):10–21, 2011. doi: 10.1016/j.conengprac.2010.08.005.

Index

active fault-tolerant system, xix, 8
analytical redundancy, xix, 12
autonomy, xix, 76
availability, xix, 175

chaser spacecraft, 2, 5, 99, 102, 103, 105, 110, 167, 175
constraint, xix, 61, 62, 123, 155, 161
control allocation, 62, 160
controlled system, xix
cross-correlation, 109, 123

decision logic, xix, 47, 122
dependability, xix, 8
disturbance, xix, 16, 23, 101, 113, 168

eigenstructure assignment, 20, 105, 137
error, xix, 19, 23, 36, 74, 78, 116, 143, 148

failure, xix, 11, 91, 105
fault, xix, 11, 98
  additive fault, 11, 16, 110, 141
  incipient fault, xx, 128, 130, 169
  multiplicative fault, 11, 98, 110
fault accommodation, xx, 10, 160
fault detection, xx, 29, 122, 140, 144
fault detector, xx, 95, 99, 110, 140
fault diagnosis, xx, 7, 91, 109, 138, 175
fault identification, xx, 50
fault isolation, xx, 48, 122, 157
fault modelling, xx, 11, 98
fault recovery, xx, 44, 93, 99, 109, 131
fault tolerance, xx, 9, 50, 69, 105, 137, 162, 163, 173
fault-tolerant control, 50, 109, 137, 161, 168

guidance, navigation and control, 1, 73, 109, 130, 176

hardware redundancy, xx, 8, 105, 131

linear matrix inequality, 19, 37, 173

model, xx, 7, 99, 102
  qualitative model, xx
  quantitative model, xx
monitoring, xx, 29, 44, 92, 93
Monte Carlo campaign, 25, 67, 125, 126, 128, 135, 167, 173

passive fault-tolerant control system, xx, 8
perturbation, xx, 22, 35, 100
propellant leakage, 3, 98, 126, 127, 166

reliability, xx
residual, xxi, 94, 110
  residual evaluation, xxi, 45, 46, 94, 122, 144
  residual generation, xxi, 25, 46, 110, 112, 141
  residual generator, xxi, 15, 140, 141

safety, xxi, 8, 92
supervision, xxi, 53
system reconfiguration, xxi, 8, 10

threshold, xxi, 25, 29, 46, 94, 122, 144
thruster configuration, 5, 62, 77, 106, 145

uncertain inertia, 145, 173, 178
uncertainty, 19, 23, 24, 38, 50, 90, 110, 113–115, 117, 145, 146, 152, 156, 170
unknown input, 16, 110, 112, 141, 143

Colophon

This dissertation was typeset with LaTeX 2_ε[2] and BibTeX by the author. The **report** document class was used and compiled using MiKTeXv2.9.4248 PC implementation of TeX/LaTeX. The body text is set 11pt with Latin Modern font which is an enhanced version of the Computer Modern font family. The manuscript has been prepared for 21 × 29.7 cm (A4) format with two-side, open-right printing.

Graphs, figures and diagrams have been produced using the following tools: MATLAB®from MathWorks Inc., Ti*k*Z - graphic system for TeX, Inkscape, and PowerPoint from Microsoft® . External sources are referenced, where applicable.

[2] LaTeX $2_\varepsilon$is an extension of LaTeX. LaTeXis a document preparation system for high-quality typesetting developed by Leslie Lamport in 1985 as a special version of Donald Knuth's TeXprogram.

Titre : Diagnostique de défaut à base de modèle et accommodation de défaut pour missions spatiales

Résumé : Les travaux de recherche traités dans cette thèse s'appuient sur l'expertise des actions menées entre l'Agence spatiale européenne (ESA), l'industrie Thales Alenia Space (TAS) et le laboratoire de l'Intégration du Matériau au Système (IMS) qui développent de nouvelles générations d'unités intégrées de guidage, navigation et pilotage (GNC) avec une fonction de détection des défauts et de tolérance des défauts. La mission de référence retenue dans cette thèse est la mission de retour d'échantillons martiens (Mars Sample Return, MSR) de l'ESA. Ce travail se concentre sur la séquence terminale du rendez-vous de la mission MSR qui correspond aux dernières centaines de mètres jusqu'à la capture. Le véhicule chasseur est l'orbiteur MSR (chasseur), alors que la cible passive est un conteneur sphérique. L'objectif au niveau de contrôle est de réaliser la capture avec une précision inférieure à quelques centimètres. Les travaux de recherche traités dans cette thèse s'intéressent au développement des approches sur base de modèle de détection et d'isolation des défauts (FDI) et de commande tolérante aux défaillances (FTC), qui pourraient augmenter d'une manière significative l'autonomie opérationnelle et fonctionnelle du chasseur pendant le rendez-vous et, d'une manière plus générale, d'un vaisseau spatial impliqué dans des missions située dans l'espace lointain. Dès lors que la redondance existe dans les capteurs et que les roues de réaction ne sont pas utilisées durant la phase de rendez-vous, le travail présenté dans cette thèse est orienté seulement vers les systèmes de propulsion par tuyères. Les défaillances examinées ont été définies conformément aux exigences de l'ESA et de TAS et suivant leurs expériences. Les approches FDI/FTC présentées s'appuient sur la redondance de capteurs, la redirection de contrôle et sur les méthodes de réallocation de contrôle, ainsi que le FDI hiérarchique, y compris les approches à base de signaux au niveau de capteurs, les approches à base de modèle de détection/localisation de défauts de propulseur et la surveillance de sécurité de trajectoire. Utilisant un simulateur industriel de haute-fidélité, les indices de performance et de fiabilité FDI, qui ont été soigneusement choisis accompagnés des campagnes de simulation de robustesse/sensibilité Monte Carlo, démontrent la viabilité des approches proposées.
Mots clés : Diagnostic des défauts; commande tolérante aux défauts rendez-vous spatial.

Title: Model-based Fault Diagnosis and Fault Accommodation for Space Missions

Abstract: The work addressed in this thesis draws expertise from actions undertaken between the European Space Agency (ESA), the industry Thales Alenia Space (TAS) and the IMS laboratory (laboratoire de l'Intégration du Matériau au Système) which develop new generations of integrated Guidance, Navigation and Control (GNC) units with fault detection and tolerance capabilities. The reference mission is the ESA's Mars Sample Return (MSR) mission. The presented work focuses on the terminal rendezvous sequence of the MSR mission which corresponds to the last few hundred meters until the capture. The chaser vehicle is the MSR Orbiter, while the passive target is a diameter spherical container. The objective at control level is a capture achievement with an accuracy better than a few centimeter. The research work addressed in this thesis is concerned by the development of model-based Fault Detection and Isolation (FDI) and Fault Tolerant Control (FTC) approaches that could significantly increase the operational and functional autonomy of the chaser during rendezvous, and more generally, of spacecraft involved in deep space missions. Since redundancy exist in the sensors and since the reaction wheels are not used during the rendezvous phase, the work presented in this thesis focuses only on the thruster-based propulsion system. The investigated faults have been defined in accordance with ESA and TAS requirements and following their experiences. The presented FDI/FTC approaches relies on hardware redundancy in sensors, control redirection and control re-allocation methods and a hierarchical FDI including signal-based approaches at sensor level, model-based approaches for thruster fault detection/isolation and trajectory safety monitoring. Carefully selected performance and reliability indices together with Monte Carlo simulation campaigns, using a high-fidelity industrial simulator, demonstrate the viability of the proposed approaches.
Keywords: Fault diagnosis; fault-tolerant control; space rendezvous.

Laboratoire de l'Intégration du Matériau au Système (IMS) - UMR CNRS 5218 - Département LAPS
Université de Bordeaux - 351 cours de la Libération - 33405 TALENCE cedex - FRANCE
http://www.ims-bordeaux.fr