

A Hierarchical Model-Based Reasoning Approach for Fault Diagnosis in Multi-Platform Space Systems

Amitabh Barua

A Thesis
in
The Department
of
Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy at
Concordia University
Montréal, Québec, Canada

December 2010

© Amitabh Barua, 2010

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: **Amitabh Barua**

Entitled: **A Hierarchical Model-Based Reasoning Approach for Fault
Diagnosis in Multi-Platform Space Systems**

and submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

complies with the regulations of this University and meets the accepted standards
with respect to originality and quality.

Signed by the final examining committee:

_____ Dr. H. Akbari, Chair
_____ Dr. T. Kirubarajan, Ext. to University
_____ Dr. F. Haghghat, Ext. to Program
_____ Dr. S. Hashtrudi Zad, Internal
_____ Dr. L. Rodrigues, Internal
_____ Dr. S. Gleason, Internal
_____ Dr. K. Khorasani, Supervisor

Approved by _____
Chair of the ECE Department

Dean of Engineering

ABSTRACT

A Hierarchical Model-Based Reasoning Approach for Fault Diagnosis in Multi-Platform Space Systems

Amitabh Barua, Ph.D.

Concordia University, 2010

Health monitoring and fault diagnosis in traditional single spacecraft missions are mostly accomplished by human operators on ground through around-the-clock monitoring and trend analysis on huge amount of telemetry data. Future multi-platform space missions, commonly known as the formation flight missions, will utilize multiple inexpensive spacecraft in formation by distributing the functionalities of a single platform among the miniature inexpensive platforms. Current spacecraft diagnosis practices do not scale up well for multiple space platforms due to an increasing need to make the long-duration missions cost-effective by limiting the size of the operations team which will be large if traditional diagnosis is employed. An ideal solution to this problem is to incorporate an autonomous fault detection, isolation, and recovery (FDIR) mechanism. However, the effectiveness of spacecraft autonomy is yet to be demonstrated and due to the existence of perceived risks, it is often desired that the expert human operators be involved in the spacecraft operations and diagnosis processes i.e., the autonomous spacecraft actions be understandable by the human operators on ground so that intervention may be made, if necessary.

To address the above problems and requirements, in this research a systematic and transparent fault diagnosis methodology for ground-based operations of multi-platform space systems is developed. First, novel hierarchical fault diagnosis concepts and framework are developed. Within this framework, a multi-platform

space system is decomposed hierarchically into multiple levels. The decomposition is driven by the need for supporting the development of the components/subsystems of the overall system by a number of design teams and performing integration at the end. A multi-platform system is considered to be a set of interacting components where components at different levels correspond to formation, system, sub-system, etc. depending on the location of the node in the hierarchy. Two directed graph based fault diagnosis models are developed namely, fuzzy rule based hierarchical fault diagnosis model (HFDM), and Bayesian networks (BN)-based component dependency model (CDM).

In HFDM, fault diagnosis of different components in the formation flight is investigated. Fuzzy rules are developed for fault diagnosis at different levels in the hierarchy by taking into account the uncertainties in the fault manifestations in a given component. In this model, the component interactions are quantified without taking the uncertainties in the component health state dependencies into account. Next, a component dependency model (CDM) based on Bayesian networks (BN) models is developed in order to take the uncertainties in component dependencies into account. A novel methodology for identifying CDM parameters is proposed. Fault evidences are introduced to the CDM when the fault modes of a component are observed via fuzzy rule activations. Advantages and limitations associated with the proposed HFDM and the CDM are also discussed. Finally, the verification and validation (V&V) of the hierarchical diagnosis models are investigated via a sensitivity analysis approach.

It should be noted that the proposed methodology and the fault diagnosis strategies and algorithms that are developed in this research are generic in a sense that they can be applied to any hierarchically decomposable complex systems. However, the system and domain specific knowledge they require, especially for modeling component dependencies, are mostly available in the aerospace industry where

extensive system design and integration-related analysis are common due to high system building cost and failure risks involved.

To my parents
Jogabrata Barua & Juthika Barua
and my wife
Aditi Das

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor Dr. K. Khorasani for the expert guidance that he has provided me during the course of this thesis. Besides providing technical comments and financial support, he has played a significant role behind my professional career development.

I would like to thank the all the committee members, especially Dr. Kirubaranjan, Dr. Rodrigues, and Dr. Gleason for all the comments and advice that they have provided. I would like to express my gratitude to Ms. Armineh Garabedian for giving me the opportunity to work for GlobVision on various space technology development projects. The experience has been very rewarding in understanding the problem that has been investigated in this thesis. I am also grateful to NSERC for supporting this research in part by a strategic research grant.

I would like to thank all my friends in Montreal as well as all the members of my research group in Concordia who made my stay at Montreal very pleasant and joyful. My special thanks go to Sadid and Faisal who have been very helpful during the thesis submission process.

Finally, I would like to express my appreciation to my wife who has been immensely patient and has provided unconditional support during this entire journey. I would also like to express my gratitude to my parents for their love, support, and continuous encouragement for higher studies throughout my life. It would not have been possible to pursue this research without the support and encouragement that I have received from my family.

TABLE OF CONTENTS

List of Figures	xii
List of Tables	xvi
List of Symbols and Abbreviations	xvii
1 Introduction	1
1.1 Spacecraft Formation Flying	1
1.2 Fault Diagnosis	4
1.3 Related Work and Motivations	8
1.4 General Problem Statement	13
1.5 Literature Review	16
1.6 Contributions of the Thesis	26
1.7 Organization of the Thesis	27
1.8 Summary	28
2 Fault Diagnosis using Fuzzy Rule-Based Reasoning and Bayesian Model-Based Reasoning	29
2.1 Fuzzy Rule-Based Fault Diagnosis	29
2.2 Bayesian Model-Based Reasoning	31
2.2.1 Probabilistic Reasoning using Bayesian Networks	31
2.2.2 Belief Updating in Bayesian Networks	33
2.2.3 Sensitivity Analysis	37
2.3 Summary	38
3 Modeling of Multi-Platform Space System and Synthetic Data Generation	39
3.1 System and Mission Parameter Selection	41
3.2 Attitude Control Subsystem (ACS)	43

3.2.1	Leader-Follower Formation Attitude Control	45
3.2.2	Subsystem Component Model	46
3.2.3	Environmental Disturbance Models	47
3.3	Electrical Power Subsystem (EPS) Model	48
3.4	Typical Simulation Results	49
3.5	Fault Simulation and Synthetic Data Generation	51
3.6	Summary	62
4	Hierarchical Fault Diagnosis Framework	64
4.1	Development of a Hierarchical Fault Diagnosis Framework	64
4.2	Level l Fault	66
4.3	Generic Directed Graph Representation	68
4.4	Fault Propagation	70
4.5	Summary	71
5	Fuzzy Rule-Based Fault Diagnosis	72
5.1	Introduction	72
5.2	Development of a Hierarchical Fault Diagnosis Model (HFDM)	73
5.2.1	HFDM Structure, Terminologies and Basic Definitions	73
5.2.2	Properties of the Proposed HFDM	78
5.2.3	Diagnosis of Faults in Independent Components at Level l	80
5.2.4	Diagnosis of Faults in Dependent Components at Level l	84
5.2.5	Rule-Based Hierarchical Fault Diagnosis	89
5.2.6	Specification of the Fuzzy Membership Functions	91
5.3	Demonstration of the Proposed Approach and Fault Diagnosis Results	93
5.4	Performance Evaluation	102
5.5	Advantages and Limitations	108
5.6	Summary	109

6	Bayesian Model-Based Fault Diagnosis	111
6.1	Introduction	111
6.2	Development of a Component Dependency Model (CDM)	113
6.2.1	Objective of the Proposed Bayesian Network Model	114
6.2.2	Proposed Bayesian Network Model Structure and Node States	115
6.2.3	Determination of Model Parameters	117
6.2.4	Evidence Generation	130
6.3	Demonstration of the Proposed Approach and Fault Diagnosis Results	132
6.4	Performance Evaluation	139
6.5	Advantages and Limitations	142
6.6	Summary	145
7	V&V of Hierarchical Fault Diagnosis	147
7.1	Introduction	147
7.2	Development of a Verification Approach for CDM	149
7.2.1	Parameter Variation in the CDM	151
7.2.2	Proposed Verification Steps	168
7.3	CDM Verification Results	170
7.4	V&V of the HFDM	178
7.5	Summary	181
8	Conclusions and Future Directions of Research	183
8.1	Concluding Remarks	183
8.2	Future Research Directions	184
8.2.1	Investigation of the CPT Generation	184
8.2.2	Investigation of the Hierarchical Agreement Factor	185
8.2.3	Investigation of the Dynamic CDM	185

8.2.4	Experimental Validation	186
8.2.5	The Cost-Benefit Analysis	186
	References	187

List of Figures

1.1	Multi-platform space missions for Earth observation and space exploration.	2
1.2	Onboard and offboard IVHM elements (adopted from [14]).	5
2.1	Belief calculation using bidirectional message passing (adopted from [55]).	35
2.2	A fragment of a poly-tree (adopted from [55]).	35
3.1	Orbits of the satellites in formation based on the special solution of the Hill's equation and its projection on ground (adopted from [128, 131]).	42
3.2	A simplified schematic diagram of a reaction wheel (adopted from [123]).	47
3.3	Functional diagram of the electrical power subsystem (EPS) (adopted from [124, 125]) depicting the locations of fault injections under the assumed EPS fault scenarios.	49
3.4	Reference attitude of the leader (Sat-1) relative to the inertial frame over 2-orbit period. In (a), the solid line represents q_1 , the dashed line represents q_2 , the dotted line represents q_3 , and the dashed-dotted line represents the constraint $\vec{q}^T \vec{q} + q_0^2 = 1$	50
3.5	Attitude (in quaternion) of the leader (Sat-1) and a follower (Sat-3) relative to the inertial frame over 2-orbit period. The solid line represents q_1 , the dashed line represents q_2 , the dotted line represents q_3 , and the dashed-dotted line represents the constraint $\vec{q}^T \vec{q} + q_0^2 = 1$.	50
3.6	Attitude error (in Euler angles) of the leader (Sat-1) and a follower (Sat-3) in the inertial frame over a 2-orbit period.	52

3.7	Relative attitude (in Euler angles) of one follower (Sat-3) with respect to the leader (Sat-1), and with respect to another follower (Sat-4) over a 2-orbit period.	53
3.8	Reaction wheel (RW) motor current of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.	54
3.9	Reaction wheel (RW) motor torque of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.	54
3.10	Reaction wheel (RW) control (torque command voltage) of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.	54
3.11	Reaction wheel (RW) speed of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.	55
3.12	Selected electrical power systems (EPS) variables of a follower (Sat-3) under healthy condition.	55
3.13	Changes of a component parameter $k(t)$ under different types of faults namely, abrupt permanent fault, abrupt intermittent fault, and non-abrupt intermittent fault.	56
3.14	The Z -axis reaction wheel (RW) torque command voltages (C_t), motor currents (I_m) and wheel speeds (ω_w) of a follower (Sat-3) in the presence of a motor current fault and a friction fault in the Z -axis reaction wheel of Sat-3 (both faults injected between $t = 7500$ s and $t = 9810$ s).	58
3.15	The X and Y axes reaction wheel (RW) torque command voltages (C_t), motor currents (I_m) and wheel speeds (ω_w) of a follower (Sat-3) in the presence of a motor current fault in the Z -axis reaction wheel of Sat-3 (injected between $t = 7500$ s and $t = 9810$ s).	59

3.16	Relative attitude (in Euler angles) of one follower (Sat-3) with respect to the leader (Sat-1), and with respect to another follower (Sat-4) in the presence of a motor current fault in the Z -axis reaction wheel of Sat-3 (injected between $t = 7500$ s and $t = 9810$ s).	60
3.17	Selected electrical power subsystem (EPS) variables of a follower (Sat-3) under a regulator fault (injected between $t = 6500$ s and $t = 6860$ s).	61
3.18	Selected electrical power subsystem (EPS) variables of a follower (Sat-3) under a battery fault (injected between $t = 6500$ s and $t = 6860$ s).	62
4.1	Proposed fault diagnosis framework for a multi-platform space system.	65
4.2	Directed graph representation of the proposed hierarchical fault diagnosis.	68
5.1	Directed graph representation of the proposed hierarchical fault diagnosis model (HFDM).	74
5.2	Decomposition of a component into “independent subcomponent” and “dependent subcomponent”.	77
5.3	A set of Gaussian membership functions representing 13-valued quantization of the diagnostic signal s_1^1 (“mean of motor current”).	93
5.4	The HFDM that resulted from a 4-level hierarchical decomposition of the formation flight of satellites as described in Chapter 3 (shown in Figure 3.1).	94
5.5	Rule activations in the Z -axis RW of Sat-3 under friction fault (the width of each bar-graph is 512 seconds).	100
5.6	Rule activations in the Z -axis RW of Sat-5 under motor current fault (the width of each bar-graph is 512 seconds).	100

5.7	Rule activations that identify a “Sat-3 fault” (the width of each bar-graph is 512 seconds).	101
5.8	Rule activations that identify a “Sat-5 fault” (the width of each bar-graph is 512 seconds).	101
5.9	Rule activations in the EPS of Sat-5 under battery fault.	102
5.10	Rule activations in the Z-axis RW of Sat-3 under low severity motor current fault (the width of each bar-graph is 512 seconds).	106
5.11	Formation level rule activations in the Sat-3 under low severity motor current fault injected at the Z-axis RW (the width of each bar-graph is 512 seconds).	107
6.1	Bayesian network representation of an L level hierarchical decomposition.	116
6.2	Health states of a child node at level l and its parent nodes at level $l - 1$	121
6.3	A 4-level Bayesian network-based component dependency model (CDM) for hierarchical fault diagnosis.	133
6.4	$P(X_3^3)$ of Sat-3 when an evidence of a fault is introduced at the subsystem component level.	139
7.1	Development and validation process of the proposed fault diagnosis models.	148
7.2	Sensitivity of Sat-3 ACS states (subsystem level) given a friction fault evidence at Sat-3 RW_y (component level).	175
7.3	Sensitivity of Sat-3 ACS states (subsystem level) given a current fault evidence at Sat-3 RW_x (component level).	176
7.4	Sensitivity of Sat-3 RW_y states (component level) given a fault evidence at Sat-3 ACS (subsystem level).	178

List of Tables

5.1	Confusion Matrix for the Subsystem Component Level	103
5.2	Confusion Matrix for the Subsystem Level	104
5.3	Confusion Matrix for the Formation (Followers) Level	104
5.4	Overall Fault Identification Accuracy	104
6.1	Performance Evaluation of the Implemented CDM	141
7.1	The Change in the Confusion Matrix at the Node C_1^{l-1} Caused Due to a Change of the Performance of the Diagnosis Algorithm Deployed at the Node	152
7.2	Confusion Matrix at Sat-3 RW-Y (C_8^1)	171
7.3	Fault Identification Accuracy Changes at Sat-3 RW-Y (C_8^1)	172

List of Symbols and Abbreviations

ABBREVIATION

AI	Artificial Intelligence
ACS	Attitude Control Subsystem
AAG	Advanced Arresting Gear
ADAPT	Advanced Diagnostics and Prognostics Testbed
AOCS	Attitude and Orbit Control Subsystem
BEAM	Beacon-based Exception Analysis for Multi-missions
BN	Bayesian Network
CBR	Case-Based Reasoning
CDM	Component Dependency Model
CPT	Conditional Probability Table
DAG	Directed Acyclic Graph
DCBR	Dynamic Case-Based Reasoning
DCM	Direction Cosine Matrix
DES	Discrete Event System
DPHM	Diagnostics, Prognostics and Health Management
DDT	Diagnostic Decision Tree
DRMD	Distributed Real-time Model-based Diagnosis
DS	Deep Space
DSS	Decision Support System
EO	Earth Observation
EOS	Earth Observing System
EPS	Electrical Power Subsystem
ESA	European Space Agency
FFT	Fast Fourier Transform
FD	Fault Diagnosis
FDI	Fault Detection and Isolation
FDIR	Fault Detection, Isolation and Recovery
FDM	Fault Diagnosis Module
FF	Formation Flying
FPA	Fault Propagation Analysis
FSM	Fault Signature Model
FIXIT	Fault Information Extraction and Investigation Tool
FMECA	Failure Mode, Effects and Criticality Analysis
GBR	Ground Based Reasoner
GNC	Guidance, Navigation and Control
HFD	Hierarchical Fault Diagnosis
HFDM	Hierarchical Fault Diagnosis Model
HMM	Hidden Markov Model

InSAR	Interferometric Synthetic Aperture Radar
IVHM	Integrated Systems Health Management
IVHM	Integrated Vehicle Health Management
LEO	Lower Earth Orbit
LF	Leader-Follower
LVLH	Local Vertical Local Horizontal
MBR	Model-Based Reasoning
MDU	Motor Driver Unit
MF	Membership Function
MI	Mode Identification
ML	Machine Learning
MPL	Model-Based Programming Language
NASA	National Aeronautics and Space Administration
NN	Neural Network
OBSW	On-Board Software
OCS	Orbit Control Subsystem
PCA	Principal Component Analysis
PDCU	Power Distribution and Control Unit
PDF	Probability Density Function
PF	Particle Filter
PEO	Planetary Environment Orbit
PID	Proportional, Integral, Derivative
RAC	Radial, Along-track, and Cross-track
RBR	Rule-Based Reasoning
RMS	Root Mean Square
RPY	Roll Pitch Yaw
RUL	Remaining Useful Life
RVM	Relevance Vector Machine
RW	Reaction Wheel
SA	Sensitivity Analysis
SOA	Software Oriented Architecture
SVM	Support Vector Machine
TPF	Terrestrial Planet Finder
V&V	Verification and Validation
VTB	Virtual Test Bed

NOMENCLATURE

List of Symbols

a	Accuracy, a coefficient in SA, semi-major axis
A	Surface area
\mathcal{A}_p^l	Set of rule synthesis assumptions at C_p^l
b	A coefficient in SA
B	Earth magnetic field
c	Element of a matrix, a coefficient in SA
\mathbf{C}_{con}	Confusion matrix
\mathbf{C}_n	The n -th one-versus-all decision matrix
C	Node or component
C_p^l	The p -th node or component at level l
C_t	Reaction wheel torque command voltage
C_d	Drag coefficient
c_g	Center of gravity
c_{pa}	Center of aerodynamic pressure
$ch(C_p^l)$	Set of child nodes of C_p^l
D	Residual dipole of a spacecraft
$D(C_p^l)$	Independent subcomponent of C_p^l
$DEP(C_p^l)$	Set of components on which C_p^l is dependent
e	Fault evidence, eccentricity
\mathbf{e}_p^l	Fault evidence introduced at p -th node at level l
f	Fault
f_k^l	The k -th fault at level l
F	Force, set of faults
F_p^l	Set of manifestable faults at the node C_p^l

$fa(C_p^l)$	The family of C_p^l
FSM_p^l	Fault signature model at the node C_p^l
\mathcal{F}	Reference frame
h	Belief adjustment factor
H	Hypothesis variable
I	Inertia, identification condition
I_m	Reaction wheel motor current
I_p^l	Identified state or fault at the node C_p^l
J	Inertia matrix
L	Link matrix
M	Magnetic moment of the Earth
$M_{n,k}^l$	Manifestations of the k -th fault in the n -th signal
$M_{p,j,k}^l$	Manifestations of the k -th fault in the signal $s_{p,j}^l$
M_p^l	Set of all fault manifestations at the node C_p^l
$M_{pq,j,k}^l$	Manifestations of the k -th fault in the signal $S_{pq,j}^l$
N_λ	Total number of initial distributions
\mathcal{O}_p^l	Set of operators at C_p^l for computing rule activation
P	Probability
$pa(C_p^l)$	Set of parent nodes of C_p^l
q	Quaternion
R	Radius of the orbit
$r_{p,k}^l$	Rule for the k faults at node C_p^l
$R_{p,K}^l$	Set of rules for the K faults at node C_p^l
s	Probability scaling parameter
S	Set of diagnostic signals
S_p^l	Set of diagnostic signals at the node C_p^l
$s_{p,j}^l$	The j -th diagnostic signal at the node C_p^l

$S_{pq,j}^l$	The j -th diagnostic signal obtained from the relative state measurements of C_p^l and C_q^l
S_{pq}^l	Set of diagnostic signals obtained from the relative state measurements of C_p^l and C_q^l
t	Time, probability scaling parameter
T	Torque experienced in polar orbit
U	Bayesian network node or state
$U(C_p^l)$	Dependent subcomponent of C_p^l
v	Diagnostic signal value
V	Set of diagnostic signal values, Bayesian network node or state, spacecraft velocity
w	weight
W	Set of weights
x	State
X	Bayesian network node or state
X_p^l	Set of states of C_p^l
Y	Bayesian network node or state
\emptyset	Empty set
α	Design parameter for membership functions, a coefficient in SA
β	A coefficient in SA
γ	User specified or recommended accuracy, a constant in SA
δ	Small change in a confusion matrix entry
ϵ	Small value
θ	Sensitivity parameter, rotation angle around Y axis
κ	A coefficient in SA

μ	Membership function, Earth's gravity constant
μ_m	Membership function corresponding to the signal value v_m
π	Parent configuration
ρ	A constant in SA, atmospheric density
ϕ	Probability potential, rotation angle around X axis
ψ	Rotation angle around Z axis
ω	Angular velocity, argument of perigee
ω_w	Reaction wheel speed
Ω	Right ascension longitude of the ascending node
$\pi(C_p^l)$	Set of predecessors of C_p^l
σ	Standard deviation
$\sigma(C_p^l)$	Set of successors of C_p^l
τ	Torque

List of Subscripts

0	Non-faulty state, inertial frame
<i>aero</i>	Aerodynamic
<i>f</i>	Fault
<i>grg</i>	Gravity
<i>i</i>	Satellite index, state index, orbit inclination
<i>id</i>	Identified
<i>j</i>	Satellite index, dummy variable
<i>J</i>	Maximum value of J
<i>k</i>	Fault index, state index, dummy variable
<i>K</i>	Maximum value of k
<i>l</i>	Level in the hierarchy

m	Diagnostic signal value index, state index
m_n	Total number of states of the n -th parent node
M	Maximum value of m
mag	Magnetic
$mean$	Mean
n	Child node's state index, state index, matrix index
N	Maximum value of N
nom	Nominal
p	Component/node index, Perigee
P	Maximum value of p
q	Component/node index
Q	Maximum value of q
$s_{p,j}^l$	The j -th diagnostic signal at the node C_p^l
$spec$	Specification
x_n	The n -th state
x	X axis
y	Y axis
z	Z axis
λ	Initial distributions

List of Superscripts

l	Level in a hierarchy
L	Maximum number of levels in a hierarchy
n	State index of a child node
p	Node or component index of a child node
T	Transpose operator

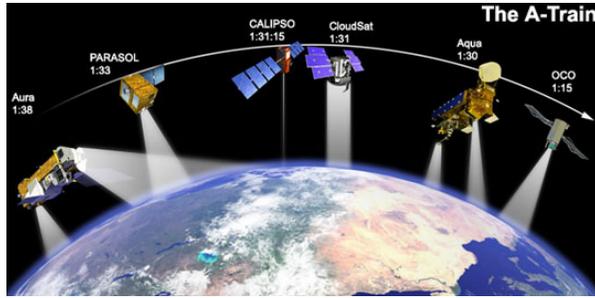
Chapter 1

Introduction

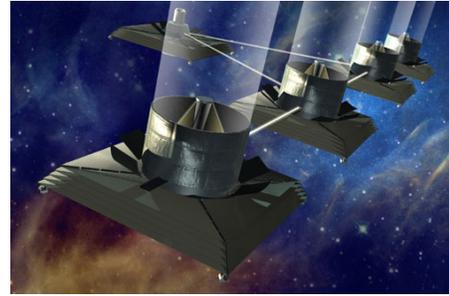
In this chapter, first a brief introduction to the general problem domain of this thesis is provided and the research motivations are presented. Next, the general problem statement and a literature review are presented. Finally, the contributions of the thesis are outlined.

1.1 Spacecraft Formation Flying

Multi-platform space systems and missions, also known as spacecraft formation flying (FF) or formation flight, is an emerging area in the Earth observation (EO) as well as space science and exploration domains. The conventional space missions utilize large, expensive spacecraft platforms. In contrast, the formation flying missions utilize multiple inexpensive spacecraft in formation by distributing the functionalities of a single platform among the miniature inexpensive platforms for achieving new capabilities in sensing objects and phenomenon in space, gathering scientific information, and sharing information among space vehicles and ground [1]. From system's point of view, the advantages of utilizing clusters of spacecraft, i.e., multiple platforms in place of an expensive single platform, are the increased robustness, flexibility, and fault tolerance, among others. However, the primary motivations for



(a) Earth observing system (EOS) [2].



(b) Terrestrial planet finder (TPF) [3].

Figure 1.1: Multi-platform space missions for Earth observation and space exploration.

formation flying come from the fact that this revolutionary concept will provide the space research community with new capabilities in sensing objects and phenomenon in space, gathering scientific information, sharing information among space vehicles and ground [1]. Based on the type of science activities that are to be performed, multi-platform missions can be grouped into two categories:

1. *Formations for Earth Observation and Planetary Exploration* [2,4]: This type of multi-platform space systems are known as planetary environment orbit (PEO) formations. In this type of formation flying missions, specialized probes are deployed with explicitly separate science objectives. The typical mission goals here are to achieve synergy of observations, synthesis of apertures for higher spacial resolution, and signal space coverage. Observation synergy involves multiple missions and multiple platforms where each platform carries specialized payloads. For example, the Earth observing system (EOS) [2] has five coordinated spacecraft as shown in Figure 1.1(a). CloudSat has a millimeter-wave radar to observe clouds and precipitation, and Calipso has a polarization-sensitive instrument for observing vertical profiles of aerosols and clouds. Each mission was designed around separate objectives, but combining signals enables answering questions such as the relationships between aerosols

and precipitation. Recently, formation flying missions for interferometric synthetic aperture radar (InSAR) applications have been proposed [5, 6]. For improved coverage over large areas, multiple Earth orbiting satellites are deployed [7–9]. However, in such missions each spacecraft is operated/controlled as an isolated entity and precise formation coordination and control are not required. Consequently, they are identified as “constellations” as opposed to “formations”.

2. *Formations for Space Science and Exploration* [3, 10–12]: This type of multi-platform space systems are known as deep space (DS) formations. In this type of missions, the idea is to build (or simulate) a large virtual telescope, typically kilometer wide, with a number of spatially separated spacecraft each carrying instruments for imaging remote objects in deep space. The formation pattern/geometry of the formation varies depending on the mission; however, each spacecraft is coordinated (in terms of position, attitude, and payload operations) with all the other members in the formation to maintain the desired formation pattern. The objective is to isolate signals that may be only milli-arcsec apart in the celestial space. Figure 1.1(b) provides an illustration of the Terrestrial Planet Finder (TPF) formation which requires very precise pointing.

It is worthwhile to mention that at present, the space community is at the initial stage in exploring the full potential of spacecraft formation flight. Some of the planned precision formation flight missions require new technologies that are not utilized in conventional spacecraft. In order to transform this vision into reality, active research is being performed in the areas of sensors and actuators development; inter-spacecraft communications; spacecraft guidance, navigation, and control (GNC); fault detection, isolation, and recovery (FDIR); computing and data management; and tools and test-beds development [13].

In this thesis, particular attention is paid on the problem of fault diagnosis in spacecraft formation flying.

1.2 Fault Diagnosis

Fault diagnosis is commonly referred to as the problem of detection, isolation, identification, or classification of faults or anomalies in the system under consideration. The overall goal of health monitoring and fault diagnosis is to detect fault(s) at early stages and to identify the location/sources of malfunction so that appropriate recovery/reconfiguration actions can be taken before the fault(s) causes a failure. Fault diagnosis is a part of a general problem area that is commonly known as Diagnostics, Prognostics and Health Management (DPHM). In this thesis, by the term “fault detection” we imply a binary decision-making about the existence of fault(s) in the system. We consider the identification/determination of the location/type/source(s) of fault in the system as “fault diagnosis” (FD). In this thesis, we use the terms “fault diagnosis” and “fault isolation” interchangeably.

Integrated Vehicle Health Management (IVHM) [14–18] refers to the integration of techniques and technologies to provide a health management system for a vehicle or fleet of vehicles. Although the requirements are unique to a specific type of vehicle, health management has become increasingly important to automotive, commercial and military aircraft, rotorcraft, unmanned and manned vehicles, spacecraft, and satellites. In the space and commercial aviation sectors, the concept of IVHM is used to describe the automation of activities that are performed onboard as well as offboard by the ground support teams and maintenance personnel. Fault diagnosis is the part of an IVHM system which aims to identify the root causes of faults and performance degradations.

Figure 1.2 shows the IVHM elements for a fleet of satellites where depending

on the desired level of onboard autonomy, diagnostic functionalities are distributed between the space and the ground segments. Within the offboard elements, a data warehouse and a ground-based reasoner (GBR) support post-processing that include health monitoring and fault diagnosis. Note that for a fleet of aircraft, it would be necessary to add an additional “maintenance” element which has very limited scope in the cases of satellites.

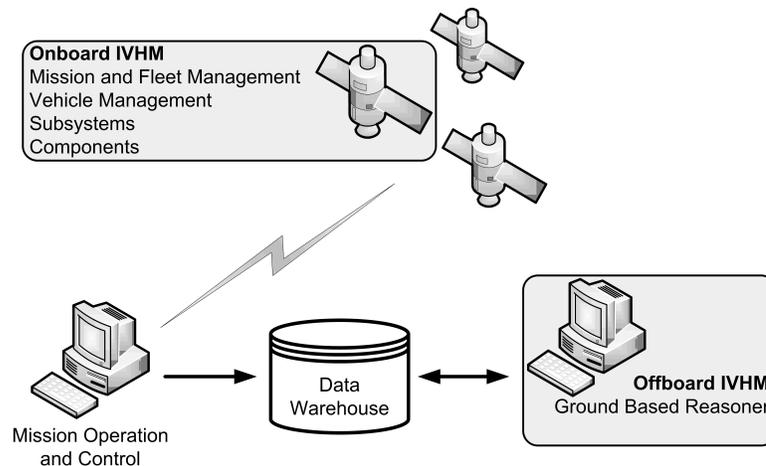


Figure 1.2: Onboard and offboard IVHM elements (adopted from [14]).

Within an IVHM framework, diagnosis of various components and subsystems are carried out by employing different types of reasoning algorithms. It is well-known within the Artificial Intelligence (AI) community that the diagnostic reasoning methods [19] are commonly classified into three main categories, namely (1) Case-Based Reasoning (CBR), (2) Rule-Based Reasoning (RBR), and (3) Model-Based Reasoning (MBR). Other approaches are mainly pure data-driven that include machine-learning (ML) and Neural Network (NN)-based strategies. The MBR approach includes graph-based models such as logical causal graph models as well as Bayesian network (BN) models. One of the fault diagnosis approaches developed in this thesis is a model-based reasoning method that utilizes a Bayesian network model which has been identified here as the Component Dependency Model (CDM).

As an alternative to the above-mentioned AI-based fault diagnosis methods, model-based fault detection and isolation (FDI) methods [20] are extensively developed and utilized by the control community. Model-based FDI methods are primarily based on precise mathematical models of the system under consideration. Based on the above discussion, fault diagnosis techniques can be broadly classified into two categories: (1) *model-based fault detection and isolation (FDI) methods*, and (2) *artificial intelligence (AI)-based or intelligent model-based fault diagnosis methods*.

In *model-based fault detection and isolation (FDI) methods*, understanding of the system from the first principles is utilized. Fault detection is performed based on residual generation and detection decisions are made by examining if the residual(s) has (have) exceed some pre-defined thresholds. For fault diagnosis, structured residuals; i.e., a set of residuals that are sensitive to a subset of faults are utilized. An *incidence table* is usually generated which is essentially a binary matrix with rows associated with residuals and columns associated with faults. This table provides a summary of which residual is sensitive to which fault. Usually, only single faults are considered in order to limit the size of this table. The fault diagnosis problem is reduced to finding a theoretical fault signature similar to the practical/actual one.

On the other hand, *artificial intelligence (AI)-based fault diagnosis methods* utilize “intelligent models” and expert human knowledge and do not require explicit mathematical models. Some of these techniques utilize numerical data while others utilize symbolic data and knowledge. Diagnosis is performed based on the knowledge and observations of much a system/component behavior is deviated from the nominal. As mentioned above, different types of computationally intelligent models and schemes such as case-based reasoning (CBR), rule-based reasoning (RBR), and model-based reasoning (MBR) are utilized depending on the depth of the available knowledge. Empirical and heuristic information as well as the experience of human experts are encoded as associative knowledge in the reasoning schemes.

Spacecraft Fault Diagnosis: There exist a variety of fault diagnosis techniques in the literature which are reviewed in Section 1.5. However, when it comes to the problem of spacecraft fault diagnosis and health monitoring, diagnostic procedures are largely dependent on human experts. Although there has been extensive research on model-based fault detection and isolation (FDI) methods in recent years, model accuracy and model-building cost are the main limitations in transferring these technologies to industries which have a more detailed information and experience with various components and subsystems. Furthermore, precise mathematical models of spacecraft systems and system components are often difficult to obtain and there are uncertainties in modeling due to incomplete understanding of the system or system component behaviors, unmodeled environmental effects, etc.

In the operations of Earth-orbiting satellites, typically large amount of telemetry data are utilized by the expert human operators located at ground stations [21]. In such cases, in the event of an anomaly, manually finding the cause and making recovery-related decisions often become a very challenging and a difficult task, if not impossible, due to the presence of a large amount of telemetry data downloaded. This approach of spacecraft diagnosis does not scale well for multiple space platform missions due to an increasing need to make the long-duration missions cost-effective by limiting the size of the operations team. Therefore, ideally the spacecraft should achieve the mission goals by autonomously carrying out fault diagnosis and recovery tasks. The need for spacecraft autonomy has been extensively discussed in the literature, and onboard planning, execution, diagnosis and recovery have been demonstrated in a deep space mission [22–25]. A framework that facilitates reducing the operational cost at the ground station for the NASA’s Deep Space Network is available in [26]. However, in the operation of the Earth-orbiting satellites the implementation of such onboard autonomous diagnosis and recovery functions and capabilities has not yet become a common practice due to cost considerations and

perceived risks. Consequently, it is often desired that expert human operators be involved in the spacecraft operations and diagnosis processes [27]. The need for efficient utilization of the telemetry data by employing machine learning and rule-based reasoning have been pointed out in [21] in order to enhance diagnostic performance and assist the less-experienced personnel in performing monitoring and diagnosis tasks.

Based on the above observations, it is therefore necessary to develop a systematic diagnosis approach for multi-platform missions in order to respond to anomalies within shortest possible time specially when critical health and safety issues are involved. The effectiveness of such a scheme is to be first demonstrated via implementation and validation as part of a ground segment automation tool (this will help limit the size of the operations team) and may be transferred on-board after a thorough feasibility analysis.

1.3 Related Work and Motivations

From the discussions on spacecraft formation flying and spacecraft fault diagnosis in Sections 1.1, and 1.2 respectively, it is important to note that there is a need and desire for the expert human operators' involvement in the spacecraft operations and diagnosis processes. In other words, spacecraft actions should be understandable by the human operators at ground so that intervention may be made, if necessary. Automated fault detection and diagnosis approaches often do not have good explanation facility to point out the source(s) of detected anomalies. This is another reason why simple and easily understandable threshold or limit checks are still preferred in satellite fault diagnosis despite the availability of much sophisticated techniques in the literature. In the remaining part of this section the works that are related to this thesis as well as the thesis motivation are discussed.

Related Work: A hierarchical Fault Detection, Isolation and Recovery (FDIR) concept for a single satellite system was presented in [28] in order to streamline and manage FDIR designs of multiple teams across a large number of spacecraft subsystems during various project phases. However, the authors in [28] present the concept mainly from the FDIR task management perspective without providing details on the systematic development of frameworks and methodologies. In [29], the authors describe the application of a model-based reasoning methodology to the health management for an Advanced Arresting Gear (AAG) system. In this work, diagnosing root causes from known symptoms is achieved by tracing upstream along the causal pathways from the symptoms to the faults. Impact prediction of root causes is performed by propagating downstream from causes to effects. The approach relies on quantitative behavioral models to detect incipient problems by simulating expected behavior and comparing against observed data. Discrepancies between predicted and observed behaviors trigger diagnosis based on qualitative fault models. These fault models capture expert diagnostic reasoning and help to isolate root causes as well as predict future impacts.

A generic hierarchical fault diagnosis approach similar to the work in this thesis is available in [19]; however, the properties of their hierarchical structure are much restrictive for applications to complex systems with multiple interactive subsystems. The purpose of the 3-level hierarchical fuzzy system model that is proposed in [30] is to model a given system with rules that are “tuned” hierarchically in 3 stages/levels. Therefore, the hierarchical decomposition goal in [30] is completely different from that of in this thesis.

The applicability of hierarchical fault diagnosis methodologies that are based on the discrete-event systems theory is available in [31]. The method in [31] is restricted to systems that are characterized by discrete events, and does not take into account uncertainties in the diagnosis model. A systems analysis method known as

the fault propagation analysis (FPA) is available in [32] that facilitates a systematic design of fault tolerant control systems by identifying all possible faults in various components and their effects on the system. The method requires an in-depth knowledge of the components interactions and serves mostly as an analysis tool for early design modifications as opposed to a tool for operational fault diagnosis which is the primary focus of this thesis. Furthermore, unlike the proposed method in this thesis, FPA does not address uncertainties in the fault manifestations at different components of the FPA model.

Rule-based reasoning have been extensively used in various applications [30, 33–41] including fault diagnosis. For example, in [37] the authors showed the effectiveness of a fuzzy logic-based fault isolation scheme on jet engines by utilizing typical gas path parameters. The author in [38] proposed an extended neuro-fuzzy scheme for online machinery condition monitoring and applied it on an experimental setup of a gearbox driven by a d.c. motor in order to classify different gear conditions. The authors in [39] proposed a rule-based diagnosis method for spacecraft that applies two different data mining techniques namely, *time-series pattern clustering* and *association rule mining* to spacecraft telemetry data.

As mentioned above, the need for efficient utilization of spacecraft telemetry data by employing machine learning and rule-based reasoning has been identified in the literature recently. The author in [40] has pointed out that when the system or the application domain is very large and complex, an entirely rule-based representation and associated inference leads to a large and inefficient knowledge base, causing a poor quality in diagnosis. The author in [40] has reported a method of data analysis intended for autonomous real-time fault detection and characterization in spacecraft by utilizing both rule-bases and causal system model without providing much details on how the models are developed and integrated.

The schemes in [37–39] appear to be suitable for the fault diagnosis of a small

set of actuators that are operated in isolation. However, there is no information available on how to utilize or employ such scheme systematically in the presence of a number of interacting components or subsystems. Eventhough a number of research on dynamic neural networks [42–46] and machine learning techniques [43, 47] have been related to the fault diagnosis of subsystem components, they do not provide details on how the methodologies can be applied in the presence of a large number of interactive components and subsystems. Furthermore, on-board design and implementation of model-based FDI methods that include parameter estimation, robust observers and filter design techniques [20, 48–51] may be cost-prohibitive for a large number of subsystems and their components even if sufficiently accurate mathematical models are available.

The methodology for quantifying the parameters of the Bayesian networks (BN) that is developed in this thesis is the result of and is being motivated by the inapplicability of the existing methods (for example, the ones in [52, 53]) to the system under consideration. The method available in [52] utilizes domain-dependent constraints that are not relevant to the problem investigated in this thesis. The method that is available in [53] is also not applicable because it was developed for ranked nodes whose states are expressed on an ordinal scale which is mapped to a continuous, monotonically ordered, bounded numerical scale. Note that several belief or evidence propagation methods in BN are available in the literature [54, 55], and the methods require that the BN parameters of the nodes be specified numerically. The focus in this thesis has been on the BN-based fault diagnosis model development (structure and parameters) as opposed to the development of a belief propagation method.

As mentioned above, although the need for spacecraft autonomy is extensively investigated in a deep space mission of NASA, in the operation of the Earth-orbiting satellites the implementation of such onboard autonomous diagnosis functions have

yet to become a common practice due to cost considerations and perceived risks.

Motivation: As mentioned in Section 1.2, fault diagnosis is considered to be an integral part of an IVHM system which aims to identify the root cause of faults and performance degradations. For complex systems such as satellites, it is often the case that different design and development teams are involved in developing diagnostic algorithms for various components and subsystems. When these algorithms are employed independently and in isolation for diagnosing a specific component or subsystem, correlating faults that are identified at separate locations will lead to difficulties in assessing the overall system health. Therefore, a decision support system should be developed that would provide the ground personnel with an ability to perform diagnostic reasoning coherently. The above observations on the limitations of the existing fault diagnosis schemes are consistent with the problems and generic fault diagnosis requirements that were encountered during the course of the industrial research and development work reported in [43] which utilized many years of actual satellite telemetry data.

The focus of this thesis is to develop a methodology for ground station-based diagnosis of complex multi-vehicle systems, such as the formation flight of satellites, where telemetry data is available and access to precise mathematical models of the system under consideration is limited. Since it is desired that the diagnosis model would provide decision support to human experts, it is reasonable to decompose the overall system into simpler subcomponents, and to develop a fault diagnosis model to relate the faults that are occurring at the subcomponents. The systematic design of such fault diagnosis scheme for satellite formations has not been investigated so far.

The above needs and limitations of the existing work have motivated the research that is pursued in this thesis. In this thesis, we develop a novel hierarchical fault diagnosis framework and methodology which allows systematic diagnostic reasoning across large number of spacecraft components or subsystems. The general idea is to decompose a complex system hierarchically into simpler modules/components, and to develop fault diagnosis models that allow the representation of module/component dependencies.

1.4 General Problem Statement

The overall research objectives are to design, develop and verify/validate fault diagnosis framework and methodologies that would enhance the level of autonomy that is achievable in ground stations, and to determine the advantages as well as limitations of the proposed approach. The problem to be addressed in this research can be formally stated as follows:

General Problem Statement

Design, implement and verify/validate a novel hierarchical fault diagnosis (HFD) scheme that is applicable for fault diagnosis in multi-platform space systems and enjoys the following properties:

- Transparent and tractable diagnostic reasoning process that is understandable by expert humans, and allows integration of FD designs performed separately by a number of design teams,
- Robust against modeling uncertainty with capability for diagnostic decision making under uncertainty, and
- Flexible for incorporating domain experts' qualitative and imprecise knowledge.

Objectives and Scope

In order to address the problem stated above, the following approach is proposed. Specifically, in order to achieve *tractability* of the diagnostic reasoning and *integration* of FD designs, it is necessary to decompose the complex system (formation flying system) into different levels of abstraction. Therefore, the first task is to develop concepts and framework for hierarchical fault diagnosis.

Once the framework is developed, the next task is to model the fault behaviors of individual components of the system at different levels in the hierarchy. Appropriate modeling schemes are to be selected that would provide *transparency* in reasoning and *robustness against modeling uncertainty*. The selected modeling scheme should also allow flexibility for *incorporation of qualitative knowledge* of the domain experts.

Next, it will be necessary to relate the fault modes/behaviors of different components and their manifestations at different levels of the proposed hierarchical framework. Therefore, it is necessary that appropriate dependency modeling of fault behaviors be performed that would allow *incorporation of imprecise knowledge* and *diagnostic decision making under uncertainty*. In summary, the following major tasks are proposed:

- Development of novel hierarchical fault diagnosis concepts and framework that would allow transparent and tractable diagnostic reasoning.
- Modeling of component fault modes and their interactions by utilizing appropriate modeling schemes that would make it possible to satisfy the requirements of the general problem stated above.
- Design and development of hierarchical fault diagnosis algorithms and strategies by utilizing the above-mentioned models.
- Verification and validation of the proposed fault diagnosis scheme.

- Identification of the advantages and the limitations of the developed fault diagnosis strategies.

In the above generic problem statement, the term “uncertainty” refers to the unclear fault manifestations in signals that are used for diagnosis as well as the misidentification of faults that is quantified typically in a standard performance matrix such as a confusion matrix [56,57]. Therefore, the term “robustness” against modeling uncertainty refers to an algorithm’s capability to identify faults by using such unclear fault manifestations, and to utilize uncertainty information that is available in confusion matrices. Furthermore, the V&V of the proposed schemes that is investigated in the thesis (in Chapter 7) provides some insights about whether the proposed scheme would break down due to some given changes in the level of uncertainty which is considered in design.

As the fault diagnosis problem under consideration is related to ground-based satellite health monitoring and fault diagnosis, the proposed schemes would not be subjected to a stringent constraint on computational resources as it would be typically the case for an on-board fault diagnosis scheme. Furthermore, the emphasis of this thesis is not on a belief propagation algorithm development (as discussed in detail in Section 6.2), and a standard belief propagation algorithm is used in the thesis to demonstrate the effectiveness of the proposed model. The computational complexity and the scalability of such standard belief propagation algorithms [54,55] are well-known, and are not investigated in this thesis.

In a well recognized recent work on the standardization of DPHM techniques, as appears in [56], fault isolation or classification accuracy of 95% within a major component for flight critical use is recommended. Therefore, in this thesis an overall fault identification accuracy across various components in the hierarchy is considered to be acceptable when it is close to 95%. Such fault identification or classification accuracy has been used as a measure of performance throughout this thesis, and

further investigation of the optimality of the proposed fault diagnosis schemes has been considered to be beyond the scope of this thesis.

Finally, the investigation on the V&V of the proposed schemes is mostly related to the verification of some generic fault diagnosis requirements as opposed to the validation of the proposed schemes with real satellite formation flight data in a real operational environment.

Main Assumptions

1. The formation control is based on Leader-follower approach.
2. Efficient fault detection mechanisms (binary decision making mechanism about the existence of fault(s)) are available that invoke or trigger the proposed fault diagnosis scheme.

The first assumption is related to the simplicity of the formation control architecture under consideration. This assumption has significant impact on the formation level (defined formally in Section 4.1) fault diagnosis rules that are proposed in Chapter 5. However, as long as the health states and their dependencies are defined in the same way as that in Chapter 6, the Bayesian network-based fault diagnosis model that is developed in this thesis would be still applicable to other formation control architectures. The second assumption simply states that the proposed fault diagnosis is invoked or initiated when deemed necessary by the user.

1.5 Literature Review

As mentioned in Section 1.2, fault diagnosis techniques for continuous-time as well as discrete-time systems can be broadly classified into two categories depending on the types of models they utilize for diagnosis: (1) *model-based fault detection and isolation (FDI) methods*, and (2) *artificial intelligence (AI)-based fault diagnosis*

methods or *intelligent model-based fault diagnosis methods*. The literature review presented below is primarily on the *artificial intelligence (AI)-based methods* since these approaches are the main focus of this research. However, for the sake of completeness, some widely used model-based fault detection and isolation (FDI) methods are also briefly reviewed.

Model-based fault detection and isolation (FDI) methods are mainly investigated within the FDI/control community. The methods [20] include *parity relation approaches*, *parameter estimation approaches*, and *observer or filter-based approaches*. The main idea behind parity relation approaches [58–60] is to check the consistency of mathematical relations between (a subset of) outputs and inputs. The parity space is the space of residuals namely, parity vectors. The overall objective of this approach is to construct a parity space for the system model under consideration and to analyze its elements for FDI. Fault detection and isolation via parameter estimation [61, 62] relies on the principle that possible faults in the monitored system are associated with specific parameters and states of the mathematical model of the system. Process parameters that are not directly measurable requires on-line parameter estimation and these parameters are utilized in the FDI. The main idea behind observer or filter-based methods [63–65] is to estimate the states of the system by using either Luenberger observer(s) or Kalman filters. A popular approach is to use a bank of estimators (Kalman filters or observers) where each estimator is designed for a specific fault hypothesis. Recent applications of the model-based diagnosis in spacecraft subsystem/component FDI are found in [48, 51, 66, 67].

The authors in [68] present a hybrid framework for fault diagnosis of complex systems that are modeled by hybrid automata where they model a residual generator by a discrete-event system (DES). The hybrid diagnosis approach is employed to investigate faults in the fuel supply system and the nozzle actuator of a single-spool turbojet engine. The authors in [69] discuss a hierarchical model-based approach

to Integrated Systems Health Management (ISHM) that combines fault detection, isolation and identification, fault-adaptive control, and prognosis into a common framework. They demonstrate the approach on a fluid loop of a secondary sodium cooling loop of a nuclear reactor system.

Model-based FDI methods are very good candidates, especially for fault detection, when the system behavior can be sufficiently approximated by a mathematical model. Note that in this case fault detection can be performed with a model of healthy system model (without explicit fault models). When it comes to the problem of diagnosis (the problem of localizing a fault, determining its type, etc.), residuals that are sensitive to a particular (set of) known faults are evaluated in order to determine what fault has occurred in the system. Therefore, as pointed out in [20], for residual evaluation/classification, model-based diagnosis approaches commonly utilize either classification techniques (statistical, geometrical, neural network-based, fuzzy clustering, etc.) or inference methods (fault symptom trees, *if-then* rules, probabilistic/fuzzy reasoning, etc.).

Artificial intelligence (AI)-based fault diagnosis methods do not require explicit mathematical models of the system; however, they utilize data and domain knowledge related to the system. As indicated in Section 1.2, AI-based diagnostic reasoning methods [19] are commonly classified into three main categories, namely (1) Case-Based Reasoning (CBR), (2) Rule-Based Reasoning (RBR), and (3) Model-Based Reasoning (MBR). Other approaches are mainly pure data-driven that include machine-learning (ML) and Neural Network (NN)-based strategies. The MBR approach includes graph-based models such as logical causal graph models as well as the Bayesian network (BN) models.

Different types of AI-based fault diagnosis methods are utilized depending on the depth of the available knowledge. When the system behavior is poorly understood, and mathematical models and/or diagnostic rules are difficult to derive,

CBR is employed. RBR is performed when it is possible for the domain experts to derive rules for diagnosis. When deep understanding of the system behavior and its component interactions are possible, and rich domain knowledge is available, MBR is employed for diagnosis. Purely data driven approaches such as neural network-based models are also utilized for diagnosis. In the subsequent paragraphs, these artificial intelligence-based techniques are reviewed.

The authors in [70] explored the use of case-based reasoning (CBR) as a technique for encoding fault management experience of the satellite operators at NASA for confronting similar anomalous situations in future. The Fault Information Extraction and Investigation Tool (FIXIT), which was implemented in the proof-of-concept form, utilized spacecraft anomaly reports to generate cases and categorized anomalies according to three levels of abstraction for performing search in the database. The authors in [71] presented a hybrid CBR architecture for integrated fault diagnosis and health maintenance of fleet of defense aviation vehicles by utilizing both textual information from maintenance records as well as sensor data. The CBR scheme in [72] was applied to fault diagnosis in spacecraft thermal subsystem by utilizing both actual and synthetic data. Simple time-domain feature extraction and time-series distance computations were utilized for case construction and retrieval. In [73], the authors identified some confidence measures in the CBR for classification of shutdown events in order to perform effective maintenance, repair, and possible design improvements of aircraft engines. CBR has also been applied to process operation support systems [74], dynamic model of a chiller system [75], online machine fault diagnosis [76], and automotive fault diagnosis [77]. The author in [78] developed a knowledge-based architecture for integrated condition based maintenance of fleet vehicles by utilizing dynamic case-based reasoning (DCBR).

Diagnostic *expert systems* that utilize rule-based reasoning have been extensively used for diagnosis in various applications. The authors in [39] proposed a

rule-based diagnosis method for spacecraft that applies two different data mining techniques namely, *time-series pattern clustering* and *association rule mining* to spacecraft telemetry data. When the system or application domain is very large and complex, an entirely rule-based representation and associated inference leads to a large and inefficient knowledge base, causing a poor quality in diagnosis. In such cases, the system is decomposed hierarchically into smaller modules and rule-bases, built for each module, are connected via a causal system model. For example, in [40] the authors describe briefly the architecture, application, and operating theory of BEAM (Beacon-based Exception Analysis for Multimissions) which is an end-to-end method of data analysis intended for real-time fault detection and characterization in spacecraft by utilizing both rule-bases and causal system model. Also, in [79] the authors discussed an architecture that allowed concurrent and cooperative processing of multiple expert systems in a hierarchical organization for real-time monitoring of spacecraft.

Fuzzy models, where the system/component behavior is represented as fuzzy *if-then* rules, are well-known for their robustness against modeling uncertainty. The authors in [80] presented a fuzzy rule-based approach for diagnosing aircraft engines where the rule base is derived by using heuristics extracted from designed experiments and flight data representing component performance changes due to field service degradation. In [37] and [81], the authors presented a fuzzy rule-based approach for aircraft engine fault isolation by utilizing gas path parameters. In [82], the authors described an expert system for gas turbine condition monitoring in which rule-based diagnostic reasoning is performed with causal graphs as well as model-based diagnosis. In [83], the authors proposed an extension to failure mode effects and criticality analysis (FMECA) for satellite fault diagnosis by utilizing fuzzy sets and causal relational methods. The authors in [84] presented a fuzzy reasoning method that allows to take various types of uncertainty between faults

and observed symptoms into account. In [85], they discussed a set of practical issues related to fault isolation in large scale industrial systems by using fuzzy reasoning methods. Applications of fuzzy rule-based reasoning are also found in fault isolation in analog circuits [86], fault diagnosis in transformers [87], fault diagnosis in benchmark actuator system [88], and diagnosis in robotic assembly lines [89].

Data driven approaches such as decision/diagnostic trees, and neural networks have been utilized for fault diagnosis when the model of the system or component under consideration is not available. In [90], the authors proposed a decision tree-based fault diagnosis scheme in which decision trees are constructed by utilizing simplified model of the process and machine-learning. The effectiveness of the scheme was demonstrated through an experimental setup of a tank-valve system. In [91], the authors proposed a fault diagnosis scheme in order to classify different states of a rotating machine by using decision trees and showed that by utilizing principal component analysis (PCA), faster tree synthesis can be achieved without compromising significant classification accuracy. However, the trees do not provide user-understandable explanation facility that is necessary in fault-cause identification and the authors pointed out that their approach had scalability issues.

In [21], the author described how data driven software tools have been applied to the NASA mission control operations and discussed plans for future mission control system health monitoring software systems. The authors in [92] used decision trees to detect and isolate simulated leaks in a rocket engine where high-fidelity simulated engine data was used to train a decision tree for fault detection and fault isolation.

The authors in [47] presented a machine learning-based automatic diagnostic tree synthesis approach in order to determine the cause of actuator faults in a satellite in terms of a set of events. However, the trees do not represent causal dependency among the events. This approach is inspired by fault-trees [93,94] which

are primarily reliability analysis models that are widely used as a failure investigation tool in aerospace industries. Generation or synthesis of fault-trees requires very good understanding and design-phase knowledge of the system, and even the software-assisted fault-tree synthesis is not time-effective for complex systems [95]. Consequently, the application of fault-tree analysis is more common in reliability analysis, failure investigations (when the system operation has come to a halt), and design verifications as compared to the operational fault diagnosis. The authors in [95] proposed a method for converting fault-trees (reliability analysis models) to decision trees (diagnostic models), denoted as the diagnostic decision trees (DDT), which allows time-effective fault diagnosis in space systems. This scheme depends on the availability of fault-trees for different parts of the system and ignores human operators' expertise/knowledge. The authors in [96] proposed an automatic health monitoring method for spacecraft which adaptively predicts the upper and the lower limits of each sensor measurement in the telemetry data by using a machine learning technique known as the regression tree learning.

The authors in [42, 44, 45] have utilized neural networks for fault diagnosis in the actuators of satellites. However, one of the main limitations of neural networks is that their diagnostic decision making process is not transparent or understandable to human experts. In order to overcome this limitation, *neuro-fuzzy* schemes are proposed for diagnosis in different applications such as d.c. motor [97], two-link rigid planar manipulator [98], etc. In [99], a computer-assisted FDI scheme based on a fuzzy qualitative simulation algorithm was used for fault detection purposes, coupled with a hierarchical structure of fuzzy neural networks that was used to perform the fault isolation task. The FDI scheme was applied to a benchmark actuator system. In [43], the authors integrated a dynamic neural network method and automatic diagnostic tree/fault tree synthesis method for fault diagnosis in the attitude control subsystem (ACS) of a satellite by utilizing actual telemetry data.

Through this integration, it has been possible to both detect faults and identify fault-causes in the ACS.

Model-based reasoning (MBR) is based on the deep knowledge of the structure and behavior of the system. In his classical paper [100] on MBR, the author presented a “constraint suspension” approach for diagnosis of digital electronic circuits. The overall strategy is based on progressive relaxation of the underlying assumptions about the correct functioning of devices that are made systematically and utilized in diagnosis. Logical causal graph-based models are also utilized in model-based reasoning. For example, the authors in [101] presented a multi-level diagnostic reasoning procedure based on causal models (*AND/OR* causal graphs). This method is developed based on sound logic without taking any uncertainty into account. In [102], authors presented an adaptive fuzzy inference causal graph approach for fault detection and isolation of field devices including sensors, actuators, and controllers in nuclear power plants. In this approach, nuclear plant systems are represented as a causal graph consisting of individual process variables that are connected with adaptive fuzzy inference system models. The authors in [103] presented a distributed, model-based, qualitative fault-diagnosis approach for formation of mobile robots. This approach is based on a bond-graph modeling framework that can deal with multiple sensor types and isolate process, sensor, and actuator faults. The authors in [104] developed a fast sensor fault diagnosis approach for component failures in large scale systems. Their approach is based on a precise and integrated statistical modeling of the fault isolation and sensor error processes where the probabilities of missed detection and of false alarms are not known a priori and must be estimated online.

Bayesian networks (BN) are used for uncertain causal dependency modeling and fault diagnosis in different applications. In [105], the authors identified BN as the most suitable computational method for spacecraft FDIR because of its ability

to process uncertain information about dependencies among system components, observation about the status of the components, effects of different alarms, etc. In [106], the authors proposed a Bayesian network-based probabilistic reasoning and statistical learning method for fault diagnosis in spacecraft thrusters by utilizing telemetry data. In [107], the authors utilized influence diagrams (generalized Bayesian networks) for fault diagnosis and decision making about corrective actions in gas turbine applications.

The authors in [108] pointed out that without systematic Bayesian network model construction techniques, BNs may never become widely used in practical diagnostic systems. They discussed systematic Bayesian network model construction by decomposing the overall problem into subproblems and representing the subproblems with simplest Bayesian networks. In [109], they proposed a large layered BN structure as a decision support tool for locomotive systems. In [110], the authors presented a novel form of layered dynamic Bayesian network model for the prognosis of electromechanical and electronic subsystems in aviation.

The authors in [111] present an uncertainty management approach for diagnostics and prognostics algorithms. In their approach, a Relevance Vector Machine (RVM), which is a Bayesian treatment of the Support Vector Machine (SVM), is used for model identification; while a Particle Filter (PF) framework uses the learnt model, statistical estimates of noise and anticipated operational conditions to provide estimates of the remaining useful life (RUL) in the form of a probability density function (PDF). The authors in [112] designed a hierarchical hybrid Bayesian network structure for information integration for security applications. In this structure, BNs are adopted in the top (decision) layer to address global assessment and hidden Markov models (HMM) functions in the bottom (observation) layer to report processed evidence to the BN. In [113], the authors presented a hierarchical system architecture for managing accountability in a service oriented architectures (SOA).

They identified root cause of service delivery failure by utilizing Bayesian network reasoning.

In [114], the authors described the “remote agent flight experiment” in which an AI-based diagnostic system namely, *Livingstone* that consists of a mode identification (MI) component was designed to perform fault diagnosis. Spacecraft components’ states were modeled as a set of discrete component modes rather than a set of low-level sensor readings. Inferred mode changes were reported to a central execution system for diagnosis and recovery. In [115], authors presented a distributed real-time model-based diagnosis (DRMD) system that combines rule-based reasoning with model-based diagnosis. DRMD utilizes *Livingstone*’s modeling language, called model-based programming language (MPL) and finds the most likely mode with a much simple algorithm as compared to that in the *Livingstone* which allows DRMD to deliver hard real-time performance. DRMD was tested on a space interferometer test-bed.

The authors in [116] discussed the issues related to the implementation of AI-based FDIR for onboard autonomy that have been identified in the SMART-FDIR project, an ESA research study. In [117], the author proposed a methodology and framework for incorporation of FDIR in on-board software (OSW) of ESA satellites. In [118], the author proposed formulation of spacecraft health management by defining six generalized health management decisions and developed a method for modeling spacecraft component dependencies. In [28], the authors presented a hierarchical FDIR framework for spacecraft systems in order to implement systematic FDIR scheme within the project development. The framework is based on the experiences from different ESA projects.

Benchmarking and standardization of diagnostic and prognostic algorithms have been investigated by several authors recently. The authors in [119] described a formal framework that was developed for benchmarking of diagnostic algorithms.

The diagnosed system is the Advanced Diagnostics and Prognostics Testbed (ADAPT), a real-world electrical power system (EPS). In [120], the author introduces several new evaluation metrics tailored for prognostics and show that the tailored metrics can effectively evaluate various algorithms as compared to other conventional metrics. The recommended practice in [56] investigated metrics that may be useful in evaluating vibration-based diagnostic algorithms as health monitors in vehicle health and usage management systems.

1.6 Contributions of the Thesis

In this thesis, a hierarchical fault diagnosis framework that allows transparent diagnostic reasoning is proposed. Within the proposed framework, the main contributions of the thesis are as follows:

1. Designed and developed a fuzzy rule-based hierarchical fault diagnosis scheme:
 - (a) Formalized the proposed fault diagnosis with a hierarchical fault diagnosis model (HFDM).
 - (b) Developed fuzzy rules for fault diagnosis in different levels in the hierarchy.
 - (c) Proposed a hierarchical fault diagnosis algorithm for identifying the faulty components in the system.
2. Designed and developed a Bayesian network-based hierarchical fault diagnosis scheme:
 - (a) Formalized the proposed fault diagnosis with a Bayesian network-based component dependency model (CDM).
 - (b) Developed a novel Bayesian network structure, and an approach for health state definition and mapping in the CDM.

- (c) Developed a novel methodology for determining CDM parameters from confusion matrix data.
3. Evaluated the performances of proposed component fault diagnosis schemes, and performed the V&V of the proposed hierarchical fault diagnosis model.
- (a) Proposed and developed a sensitivity analysis-based CDM verification approach.
 - (b) Demonstrated the verification of the CDM that is implemented in this thesis.

In addition, the advantages and the limitations of the developed fault diagnosis schemes in items 1 and 2 above have been identified.

1.7 Organization of the Thesis

The organization of the remaining parts of this thesis is as follows: In Chapter 2, the background information that are utilized in this thesis are briefly reviewed. In Chapter 3, the modeling of a formation flight system and formation flight synthetic data generation are discussed. In Chapter 4, the proposed hierarchical framework for satellites formation flight fault diagnosis is discussed in detail. In Chapter 5, the proposed hierarchical fault diagnosis framework is formalized and a fuzzy rule-based fault diagnosis methodology within the proposed framework is presented. In Chapter 6, a Bayesian network-based fault diagnosis methodology is investigated and developed. In Chapter 7, the verification and validation of the above fault diagnosis schemes are investigated. Finally, conclusions and future work are stated in Chapter 8.

1.8 Summary

In this chapter, the state-of-the-art on multi-platform space missions namely, spacecraft formation flying missions, spacecraft fault diagnosis and spacecraft autonomy are discussed. The problem of multi-platform space systems fault diagnosis, which is the focus of this research, is discussed and motivations for pursuing this research are outlined. Next, the thesis contributions are summarized, and the organization of the thesis is presented. Finally, an extensive literature review on fault diagnosis methodologies, with an emphasis on the artificial intelligence (AI)-based fault diagnosis methods is presented.

Chapter 2

Fault Diagnosis using Fuzzy Rule-Based Reasoning and Bayesian Model-Based Reasoning

In this chapter the methodologies that are necessary for this research are briefly reviewed and discussed.

2.1 Fuzzy Rule-Based Fault Diagnosis

In this section, a brief review of fuzzy reasoning-based fault isolation is discussed based on the formulation available in [19, 84, 85]. For fault isolation in physical systems, relationships among observed symptoms and faults is necessary. Symptoms are the manifestation of faults available diagnostic signals (measured from the process or calculated). Therefore, symptoms are obtained by monitoring some pre-identified diagnostic signals that are of one of the following types [19]: (1) residuals generated based on system models, (2) binary or multi-valued signals resulted from residual classification/quantification, (3) statistical parameters (features) describing signal properties, and (4) process states and/or variables (measured or calculated).

Let $F = \{f_k : k = 1, \dots, K\}$ be a finite set of K faults under consideration and $S = \{s_j : j = 1, \dots, J\}$ be a finite set of J available diagnostic signals. Each diagnostic signal $s_j \in S$ can then have a set of possible values M_j where, $M_j = \{m_{j,a}, m_{j,b}, \dots, m_{j,z}\}$, called the domain of s_j , is a fuzzy set with fuzzy/linguistic variables $m_{j,a}, m_{j,b}, \dots, etc.$. Note that the number of variables in M_j for each s_j need not necessarily be the same. In practice, usually two- or three-valued signals are considered for simplicity; for example, $M_j = \{m_{j,a}, m_{j,b}, m_{j,c}\}$ for a three-valued diagnostic signal $s_j \in S$. Consequently, for each value m_j , a membership function $\mu(m_j) \in (0, 1)$ is determined which essentially represents the degree of truth that the value of s_j is m_j .

A mapping $S \times F \rightarrow M$ is defined which assigns to each pair $\langle s_j, f_k \rangle$ a subset of the values $M_{j,k} \subset M_j$. Note that $M_{j,k}$ are the possible values (considered as manifestations) of s_j when fault f_k occurs. A fault signature model (FSM), with matrix representation $M(f_k)$ is constructed in which the k -th column of M is called the signature of the fault f_k :

$$M = \begin{pmatrix} M_{1,1} & \dots & M_{1,K} \\ \dots & M_{j,k} & \dots \\ M_{J,1} & \dots & M_{J,K} \end{pmatrix} \quad (2.1)$$

Note that the k -th column of M represents a *complex signature* that may consist of multiple elementary signatures (refer to [19, 84] for detail). Relationships among faults and symptoms are expressed in the form of *if-then* rules such as:

$$\text{If } (s_1 \in M_{1,k}) \text{ and... } (s_j \in M_{j,k}) \text{ ...and } (s_J \in M_{J,k}) \text{ then } (f_k) \quad (2.2)$$

Complex premise fulfillment factor is determined as follows:

$$\mu(s_j \in M_{j,k}) = \mu(s_j \in m_{j,1}) \oplus \mu(s_j \in m_{j,2}) \dots \oplus \mu(s_j \in m_{j,n}) \quad (2.3)$$

for n-valued evaluation of s_j . The symbol \oplus represents fuzzy sum operator, for example, s -norm operators such as MAX or drastic sum (refer to [121] for further detail on the operator). The activation level for the rule for k -th fault is given by:

$$\mu(f_k) = \mu(s_1 \in M_{1,k}) \otimes \dots (s_j \in M_{j,k}) \otimes \dots (s_J \in M_{J,k}) \quad (2.4)$$

where the symbol \otimes represents fuzzy conjunction operator, for example, t -norm operators such as MIN or PROD (refer to [19, 121] for further detail on the operators). Diagnosis is formulated on the basis of rule activation level. Identified faults usually have rule activation level higher than some pre-defined fixed threshold value H , which is available from expert knowledge and/or through observation of nominal activation due to the presence of noise and disturbances acting on the system according to:

$$F_{isolated} = \{f_k : \mu(f_k) > H\} \quad (2.5)$$

2.2 Bayesian Model-Based Reasoning

A brief background study on Bayesian networks is provided in Sections 2.2.1 and 2.2.3. The reviews in the subsequent sections are based on [54], [122], and [55].

2.2.1 Probabilistic Reasoning using Bayesian Networks

Bayesian inference is based on the “degree of belief” interpretation of probability as opposed to *classical statistical inference* which is based on a long-run frequency interpretation of probability. The heart of Bayesian techniques lies in the celebrated inversion formula:

$$P(X|e) = \frac{P(e|X)P(X)}{P(e)} \quad (2.6)$$

which states that the belief about a hypothesis X upon obtaining evidence e can be computed by multiplying previous belief $P(X)$ by the likelihood $P(e|X)$ that e will materialize if X is true. $P(X|e)$ is called the *posterior* probability, and $P(X)$ is the *prior* probability. The denominator is merely a normalizing constant $P(e) = P(e|X)P(X) + P(e|\neg X)P(\neg X)$, which can be computed by requiring that $P(X|e)$ and $P(\neg X|e)$ sum to unity. Equation (2.6) is regarded as a normative rule for updating beliefs in response to evidence.

A Bayesian network (BN) consists of the following: A set of *variables* and a set of *directed edges* between variables; where each variable has a finite set of mutually exclusive states, are characterized so that the variables together with the directed edges form a *directed acyclic graph* (DAG). To each variable X_i , with parents U_1, U_2, \dots, U_n there is a attached conditional probability distribution $P(X_i|U_1, \dots, U_n)$. For a BN over $X = \{X_1, \dots, X_n\}$, the joint probability distribution $P(X)$ is the product of all conditional probabilities specified in BN:

$$P(X) = \prod_i P(X_i|pa(X_i)) \quad (2.7)$$

where, $pa(X_i)$ is the parent set of X_i .

Let BN be a Bayesian network over the universe of variables \mathcal{U} , and let a_i , where $i = 1, 2, \dots, n$, be a state of $A \in \mathcal{U}$ and b_j , where $j = 1, 2, \dots, m$, be a state of $B \in \mathcal{U}$. The probability of observing joint outcomes is expressed by *joint probability*. The joint probability table $P(A, B)$ consists of $n.m$ numbers and is represented in an $n \times m$ table. From a joint probability table $P(A, B)$, the probability $P(A)$ is calculated as follows:

$$P(a_i) = \sum_1^m P(a_i, b_j) \quad (2.8)$$

This calculation is called *marginalization*, and we say that the variable B is marginalized out of $P(A, B)$, thus resulting in $P(A)$. The widely used notation

is as follows:

$$P(A) = \sum_B P(A, B)$$

Probability Potentials

Multiplication and marginalization of tables are possible. The tables need not be (conditional) probabilities, and they are generally called *potentials*. A potential ϕ is a real-valued function over a domain of finite variables \mathcal{X} :

$$\phi : sp(\mathcal{X}) \rightarrow \mathbb{R}$$

where $sp(\mathcal{X})$ is the span of \mathcal{X} . The domain of a potential is denoted by $dom(\phi)$. For example, the domain of the potential $\phi(A, B|C)$ is $dom(\phi(A, B|C)) = \{A, B, C\}$.

Two potentials can be multiplied, and the multiplication has several properties that include $dom(\phi_1, \phi_2) = dom(\phi_1) \cup dom(\phi_2)$ in addition to *commutative law*, *associative law*, and *distributive law*, *existence of unit potential* properties (refer to [55] for details).

The marginalization can be generalized to potentials so that $\sum_A \phi$ is a potential over $dom(\phi) \setminus \{A\}$. Marginalization is *commutative*:

$$\sum_A \sum_B \phi = \sum_B \sum_A \phi$$

2.2.2 Belief Updating in Bayesian Networks

In this section belief/information propagation and belief updating in Bayesian networks are reviewed. Various information propagation methods that are available in the literature are discussed in [55] (in Chapter 4). In the subsequent paragraphs, belief updating in *causal poly-tree* type Bayesian networks is reviewed.

Belief Updating by Unidirectional Information Propagation

In a simple tree structured network with two nodes and one link, $X \rightarrow Y$, the

directed link is quantified by a conditional probability distribution or a fixed conditional probability matrix $M_{Y|X}$ in the discrete case:

$$M_{Y|X} \triangleq P(Y|X) = \begin{pmatrix} P(y_1|x_1) & \dots & P(y_N|x_1) \\ \dots & P(y_n|x_m) & \dots \\ P(y_1|x_M) & \dots & P(y_N|x_M) \end{pmatrix} \quad (2.9)$$

If an evidence $\mathbf{e}^- = \{Y = y\}$ is observed, then from Baye's rule, the belief distribution of X is given by:

$$BEL(X) \triangleq P(X|\mathbf{e}^-) = \alpha P(X)\lambda(X) \quad (2.10)$$

where, $\alpha = [P(\mathbf{e}^-)]^{-1}$ is a normalizing constant, $P(X)$ is the prior probability of X , and $\lambda(X)$ is the likelihood vector or *diagnostic support contributed by the child* which corresponds to the y 's column of the link matrix $M_{Y|X}$, namely:

$$\lambda(X) = P(\mathbf{e}^-|X) = P(Y = y|X) = M_{Y|X} \quad (2.11)$$

If Y is not observed directly but supported by an indirect observation $\mathbf{e}^- = \{Z = y\}$ in a chain $X \rightarrow Y \rightarrow Z$, then

$$\begin{aligned} \lambda(X) &= P(\mathbf{e}^-|X) = \sum_y P(\mathbf{e}^-|Y, X) = \sum_y P(\mathbf{e}^-|Y)P(Y|X) \\ &= M_{Y|X}\lambda(Y) \end{aligned} \quad (2.12)$$

Belief Updating by Bidirectional Information Propagation

Let a chain be $\mathbf{e}^+ \rightarrow T \rightarrow U \rightarrow X \rightarrow Y \rightarrow Z \rightarrow \mathbf{e}^-$ as shown in Figure 2.1; where \mathbf{e}^+ and \mathbf{e}^- are the evidences connected to X through its parent U and child Y , respectively. The impacts of \mathbf{e}^+ and \mathbf{e}^- on X are expressed in two separate vectors $\pi(X) = P(X|\mathbf{e}^+)$ and $\lambda(X) = P(\mathbf{e}^-|X)$; where, $\lambda(X)$ is called the *diagnostic support contributed by child* (as above), and $\pi(X)$ is called the *causal support contributed by*

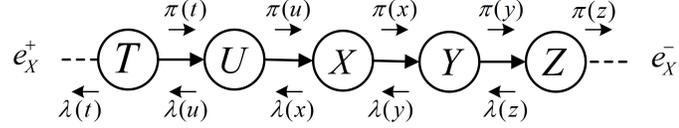


Figure 2.1: Belief calculation using bidirectional message passing (adopted from [55]).

parent, where

$$\begin{aligned}
 BEL(X) &\triangleq P(X|\mathbf{e}^-, \mathbf{e}^+) = \alpha P(\mathbf{e}^-|X, \mathbf{e}^+)P(X|\mathbf{e}^+) \\
 &= \alpha P(\mathbf{e}^-|X)P(X|\mathbf{e}^+) = \alpha \lambda(X)\pi(X)
 \end{aligned} \tag{2.13}$$

which is identical to Equation (2.10) with $\pi(X)$ replacing the prior probability $P(X)$.

Conditioning $\pi(X) = P(X|\mathbf{e}^+)$ on the parent variable U we obtain:

$$\begin{aligned}
 \pi(X) &= P(X|\mathbf{e}^+) = \sum_u P(X|U, \mathbf{e}^+)P(U|\mathbf{e}^+) = \sum_u P(X|U)\pi(U) \\
 &= \pi(U)M_{X|U}
 \end{aligned} \tag{2.14}$$

Therefore, from Equations (2.12, 2.13, 2.14) it is observed that in order to compute belief distribution $BEL(X)$, a node requires $\pi(U)$ of its parent and $\lambda(X)$ of its child.

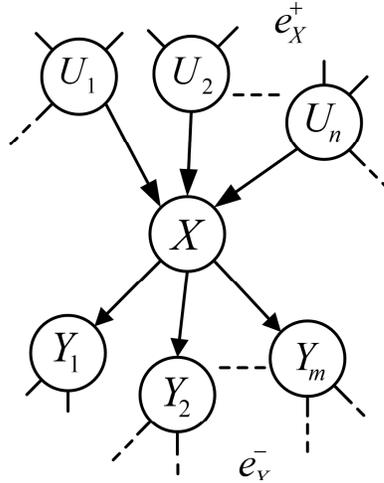


Figure 2.2: A fragment of a poly-tree (adopted from [55]).

Now, consider a fragment of a poly-tree (the tree is *singly connected* namely, no

more than one path exists between any two nodes, as shown in Figure 2.2) consisting of a node X , the set of all X 's parents, $\mathbf{U} = \{U_1, U_2, \dots, U_n\}$, and the set of all X 's children $\mathbf{Y} = \{Y_1, Y_2, \dots, Y_m\}$. Let \mathbf{e} be the total evidence obtained, \mathbf{e}_X^- be the evidence connected to X through its children \mathbf{Y} , and \mathbf{e}_X^+ be the evidence connected to X through its parents \mathbf{U} . Moreover, \mathbf{e}_X^- and \mathbf{e}_X^+ are further decomposed into $\mathbf{e}_X^- = \{\mathbf{e}_{XY_1}^-, \mathbf{e}_{XY_2}^-, \dots, \mathbf{e}_{XY_m}^-\}$ and $\mathbf{e}_X^+ = \{\mathbf{e}_{U_1X}^+, \mathbf{e}_{U_2X}^+, \dots, \mathbf{e}_{U_nX}^+\}$, respectively.

Incoming information to X are: $\lambda_{Y_j}(X) : j = 1, 2, \dots, m$ and $\pi_X(U_i) : i = 1, 2, \dots, n$. Outgoing information from X are: $\lambda_X(U_i) : i = 1, 2, \dots, n$ and $\pi_{Y_j}(X) : j = 1, 2, \dots, m$. Stored information is the fixed conditional probability matrix $P(X|U_1, U_2, \dots, U_n)$ that relates X to its immediate parents. Utilizing the incoming information, at X , $\lambda(X)$ and $\pi(X)$ are computed so that the belief distribution $BEL(X)$ can be obtained according to:

$$\begin{aligned} \lambda(X) &\triangleq P(\mathbf{e}_X^-|X) = P(\mathbf{e}_{XY_1}^-, \dots, \mathbf{e}_{XY_m}^-|X) = P(\mathbf{e}_{XY_1}^-|X) \dots P(\mathbf{e}_{XY_m}^-|X) \\ &= \prod_{j=1}^m \lambda_{Y_j}(X) \end{aligned} \quad (2.15)$$

$$\begin{aligned} \pi(X) &\triangleq P(X|\mathbf{e}_X^+) = \sum_{U_1, \dots, U_n} P(X|U_1, \dots, U_n) P(U_1|\mathbf{e}_{U_1X}^+) \dots P(U_n|\mathbf{e}_{U_nX}^+) \\ &= \sum_{U_1, \dots, U_n} P(X|U_1, \dots, U_n) \pi_X(U_1) \dots \pi_X(U_n) \\ &= \sum_{U_1, \dots, U_n} P(X|\mathbf{U}) \prod_{i=1}^n \pi_X(U_i) \end{aligned} \quad (2.16)$$

The outgoing information from X are computed as follows:

$$\lambda_X(U_i) = \beta \sum_X \lambda(X) \sum_{U_k: k \neq i} P(X|U_1, \dots, U_n) \prod_{k \neq i} \pi_X(U_k) \quad (2.17)$$

$$\pi_{Y_j}(X) = \alpha \prod_{k \neq j} \lambda_{Y_k}(X) \pi(X) \quad (2.18)$$

2.2.3 Sensitivity Analysis

Let BN be a Bayesian network with evidence e . Assume that there is a single hypothesis variable H , and let a particular state h of H be in focus of interest. Let \mathbf{t} be a set of parameters of the BN (a parameter is an entry in a conditional probability table (CPT)). One is interested to know how $P(h|e)$ varies with \mathbf{t} . Therefore, the probabilities must be expressed as the functions of the parameters which is discussed next for a binary variable.

Let X be a binary variable, and let π be a configuration of X 's parents $pa(X)$. Then $t = P(X = x|\pi)$ is a parameter (an entry in a CPT), but consequently $P(X = \bar{x}|\pi) = 1 - t$ co-varies with t . If X has more than two states, *proportional scaling* is assumed, that is the remaining probabilities are scaled by the same factor. If X has n states, and x_1 is a parameterized state, it is assumed that $P(X|\pi) = (t, (1 - t)x_2, \dots, (1 - t)x_n)$, where $\sum x_i = 1$. It is possible to deal with several parameters in the same distribution. If, for example, the first two states are parameterized, one would require $P(X|\pi) = (t, s, (1 - t - s)x_3, \dots, (1 - t - s)x_n)$. Then, s does not scale when t is changed. The following assumes proportional scaling, and at most one parameter per distribution.

Theorem 2.2.1 (*$P(e)$ as a function of a parameter* [55]). Let BN be a Bayesian network over the universe of variables \mathcal{U} . Let t be a parameter and let e be evidence entered in BN . Then assuming proportional scaling, we have $P(e)(t) = \alpha t + \beta$; where α and β are real numbers.

Let $\mathbf{t} = (t_1, \dots, t_m)$ be a set of parameters, and let $pol(\mathbf{t})$ be a polynomial over \mathbf{t} . The polynomial $pol(\mathbf{t})$ is said to be *multilinear* if all exponents in the expression are of degree at most 1. If so, it has a term for each subset of \mathbf{t} .

Corollary 2.2.1 ($P(e)(\mathbf{t})$ is multilinear [55]). Let BN be a Bayesian network over the universe of variables \mathcal{U} . Let \mathbf{t} be a set of parameters for different distributions and let e be evidence entered to BN . Then assuming proportional scaling, $P(e)(\mathbf{t})$ is a multilinear polynomial over \mathbf{t} .

Corollary 2.2.2 ($P(h|e)(\mathbf{t})$ is a fraction of multilinear polynomials [55]). Let BN be a Bayesian network over the universe of variables \mathcal{U} . Let \mathbf{t} be a set of parameters for different distributions and let x be a state of $X \in \mathcal{U}$ and let e be evidence. Then $P(h|e)(\mathbf{t})$ is a fraction of two multilinear polynomials over \mathbf{t} .

For a parameter t , Corollary 2.2.2 yields that $P(h|e)$ has the form

$$P(h|e) = \frac{\alpha t + \beta}{at + b} = \frac{P(h, e)}{P(e)} \quad (2.19)$$

2.3 Summary

In this chapter, background information that are necessary for this research are provided. The topics include fuzzy rule-based fault diagnosis, and probabilistic reasoning using Bayesian networks.

Chapter 3

Modeling of Multi-Platform Space System and Synthetic Data Generation

In this thesis synthetic formation flight data has been utilized in order to demonstrate the effectiveness of the fault diagnosis schemes that are developed and to evaluate the performances of the fault diagnosis schemes. Note that utilization of synthetic formation flying system data has been necessary due to the unavailability of actual telemetry data from multi-platform or formation flight space missions which are still mostly in the planning and design stages. First, description of the data generation model is provided in the subsequent paragraphs and sections.

A satellite consists of a number of interacting subsystems. In this thesis, the focus is only on some selected subsystems. Primarily, faults that are related to the attitude control subsystem (ACS) actuators are investigated; specifically the reaction wheel actuators. For this purpose, sufficiently accurate ACSs with a “Leader-Follower” formation control architecture with high-fidelity subsystem components/actuator models have been implemented. In addition, a simplified satellite

electrical power subsystem (EPS) model has been utilized. The following are the characteristics and assumptions that are associated with the implemented leader-follower formation flight simulation model:

- Attitude control is not coupled with orbital control, and the satellites' reference attitude (desired attitude manoeuvres) as well as the external disturbances are computed and specified based on the following assumptions:
 - The leader is in a Keplerian orbit, orbit type: LEO, altitude 550 *km* (refer to Section 3.1 for details)
 - The followers follow an elliptical orbit around the leader, and maintain the same attitude with respect to the leader (refer to Sections 3.1 and 3.2 for details)
- Attitude controllers are designed for each axis based on PID control laws (refer to Section 3.2.1)
- A high fidelity reaction wheel actuator [123] model is implemented that includes motor driver/torque control mechanism, motor disturbances such as cogging and ripple torques, Coulomb and viscous friction, torque noise that results due to lubricant dynamics, and EMF torque limiting (refer to Section 3.2.2)
- Ideal attitude sensor dynamics is assumed
- Worst-case environmental disturbances are assumed: cyclic magnetic torque and constant gravity gradient and aerodynamic torque are applied (refer to Section 3.2.3)
- Virtual test bed (VTB) [124, 125] simulation is used to generate EPS data

- VTB includes a solar array illumination model, a solar array model, a controller or simplified power distribution and control unit (PDCU), a battery model, and a voltage regulator
- EPS data is generated by setting the assumed orbital characteristics as mentioned above
- Pre-generated EPS data is fed to ACS which implies that the EPS behavior impacts the ACS but the converse is not true (refer to Section 3.3 for details)

In the subsequent sections, the ACS and the EPS models that are utilized for synthetic fault data generation are discussed in some detail.

3.1 System and Mission Parameter Selection

The primary interest of this research is on the faults that are related to the ACS and the EPS of satellites in a formation flight. The orbital control subsystem (OCS), in general, has significant impact on the ACS of a satellite. However, for faults at steady state conditions, it is reasonable to assume that the two subsystems are decoupled. Furthermore, in order to generate reference attitude states for individual satellites in the formation, it is necessary to know the orbital parameters (desired orbit altitude, orbit inclination, etc.) as well as the desired formation geometry or the desired relative position of the satellites in the formation even though one assumes that spacecraft orbital dynamics is decoupled from its attitude dynamics. Furthermore, orbit characteristics play a significant role in determining worst-case attitude disturbance torques. In this research planetary environment orbit (PEO) formations are considered. PEO formations for scientific observation synergy as well as interferometric synthetic aperture radar (InSAR) applications often require to maintain fixed formation configuration/pattern [5, 6, 126]. In the case of circular orbits with inter-spacecraft separation distances less than 1 km, it is possible to

derive a closed form relative motion equations known as the Clohessy-Whitshire or the Hill's equations [127]. Assuming that the Leader satellite is in a Keplerian orbit, the “special class of periodic solution” of Hill's equation provide orbits for each follower relative to the Leader [128]. Based on the information available in [6, 129], it is reasonable to assume a Sun-synchronous Low Earth Orbit (LEO) with 550 km altitude (orbital period: 95 min (approx.)); i.e., the orbital specification in terms of the six classical orbital elements [130] for the leader satellite is as follows: semi-major axis, $a = 6928$ km; eccentricity, $e = 0$ (circular orbit); time of perigee passage, $t_p = 0$ s; right ascension longitude of the ascending node $\Omega = 0$ degrees; inclination of the orbit plane, $i = 97.5$ degrees; and argument of perigee, $\omega = 0$ degree. It is

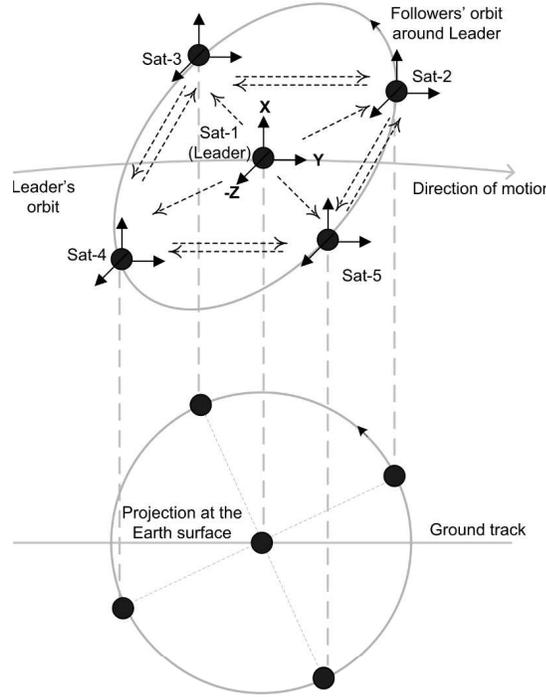


Figure 3.1: Orbits of the satellites in formation based on the special solution of the Hill's equation and its projection on ground (adopted from [128, 131]).

further assumed that the follower satellites' desired orbits are specified by utilizing the solutions of Hill's equations (as available in [128]) and the followers circle the Leader satellite in an elliptical orbit such that the projection of this ellipse on the ground (area covered on the ground) has a circular shape with a desired radius of

800 m as shown in Figure 3.1. For case study, a formation of 5 (five) satellites is considered where a dotted arrow in Figure 3.1 from satellite- j to satellite- i indicates that attitude of satellite- i can be obtained with respect to satellite- j . Though it is possible to employ big satellites (with approx. 1000 kg mass) in formation-flying mission, tight formation flying (inter-satellite distance less than 1 km) of small satellites is considered in this thesis. Therefore, based on the information available in [132], mass of each satellite has been selected as 100 kg with principal moment of inertia $[I_{xx}, I_{yy}, I_{zz}] = [5, 5, 4] kg\cdot m^2$. It is assumed, for the sake of simplicity and without loss of generality, that all the satellites in the formation have identical mass and inertia.

3.2 Attitude Control Subsystem (ACS)

In general, in this research a formation of satellites with a single leader and n followers is considered. Three coordinate frames are used, namely: (1) a reference frame \mathcal{F}_0 is used as an inertial frame whose origin is at the center of the Earth, (2) a reference frame \mathcal{F}_L embedded at the center of mass of the leader as a body frame which rotates with the spacecraft and represents its orientation, and (3) a local vertical local horizontal (LVLH) reference frame \mathcal{F}_i attached to the orbit of each satellite. The RAC-reference frame is used as a spacecraft-centered frame (as opposed to the roll, pitch, yaw (RPY) frame) in which x, y, z coordinates correspond to *radial*, *along-track* (direction of motion), and *cross-track* (perpendicular to orbit plane) directions, respectively.

Attitude of a satellite can be represented in different ways with sets of variables such as the Euler angles, direction cosine matrix (DCM), Euler parameters (sometimes called *quaternion*), etc. Euler angles consist of three successive rotation angles (ϕ, θ, ψ) around the x, y, z axes of satellite's body frame. The main advantage of

the Euler angle representation is that it provides easy visualization of the rotations and orientation of the satellite. Despite its advantages, the presence of singularities at specific angles limits applicability of the Euler angle representation to small rotations. For this reason, in this thesis, quaternion representation [133, 134] is utilized for spacecraft attitude. An angular displacement can be specified by the *Euler parameters* or unit *quaternion* $\bar{q} = (\vec{q}, q_0)$ which is defined as: $\vec{q} = [q_1, q_2, q_3]^T \triangleq \vec{a} \cdot \sin \frac{\phi}{2}$ and the auxiliary parameter $q_0 \triangleq \cos \frac{\phi}{2}$. In this notation, \vec{a} is a unit vector in the direction of rotation with coordinate representation $[a_1, a_2, a_3]^T$, called *eigenaxis*, and ϕ is the rotation angle about \vec{a} . By definition, unit quaternion is subject to the constraint that $\vec{q}^T \vec{q} + q_0^2 = 1$. Note that a unit quaternion is not unique since \bar{q} and $-\bar{q}$ represent the same attitude. However, uniqueness can be achieved by restricting ϕ to $0 \leq \phi \leq \pi$ so that $q_0 \geq 0$.

Furthermore, given a vector $\vec{v} = [v_1, v_2, v_3]^T$, the cross product operator is denoted by:

$$\vec{v}^\times = \begin{bmatrix} 0 & -v_3 & v_2 \\ v_3 & 0 & -v_1 \\ -v_2 & v_1 & 0 \end{bmatrix} \quad (3.1)$$

which represents the fact that $\vec{v} \times \vec{\omega} = \vec{v}^\times \vec{\omega}$. The product of two unit quaternion \bar{p} and \bar{q} is defined as:

$$\bar{p}\bar{q} = \begin{bmatrix} q_0\vec{p} + p_0\vec{q} + \vec{q} \times \vec{p} \\ q_0p_0 - \vec{q}^T \vec{p} \end{bmatrix} \quad (3.2)$$

which is a unit quaternion as well. The conjugate of \bar{q} is defined as $q^\star = [-\vec{q}^T, q_0]^T$. The multiplicative identity quaternion is denoted by $\mathbf{1} = [0, 0, 0, 1]^T$, where, $q^\star \bar{q} = \bar{q} q^\star = \mathbf{1}$ and $\bar{q}\mathbf{1} = \mathbf{1}\bar{q} = \bar{q}$. If \bar{q}^d and \bar{q} represent desired and actual attitude respectively, then the attitude error is given by $\bar{q}_e = \bar{q}^{d\star} \bar{q}$, which represents the attitude of the actual frame \mathcal{F} with respect to the desired frame \mathcal{F}^d . Finally, the

rotational dynamics of a spacecraft relative to the inertial frame \mathcal{F}_0 are as follows:

$$\begin{aligned}
 \dot{\vec{q}} &= -\frac{1}{2}\vec{\omega} \times \vec{q} + \frac{1}{2}q_0\vec{\omega} \\
 \dot{q}_0 &= -\frac{1}{2}\vec{\omega} \cdot \vec{q} \\
 J\dot{\vec{\omega}} &= -\vec{\omega} \times (J\vec{\omega}) + \vec{\tau}
 \end{aligned} \tag{3.3}$$

where, $\vec{\omega} = [\omega_x, \omega_y, \omega_z]^T$ represents the angular velocity of the satellite, \vec{q} is the vector and q_0 is the scalar part of the quaternion, J is the inertia matrix and $\tau = [\tau_x, \tau_y, \tau_z]^T$ are the torques associated with the spacecraft.

3.2.1 Leader-Follower Formation Attitude Control

It is assumed in this thesis that the 5 (five) satellites in the formation under the assumed mission scenario (as discussed in Section 3.1) would perform synchronous/collaborative attitude maneuvers. Since the follower satellites circle around the Leader at the orbital rate, in order to ensure contact or line-of-sight with the followers, the leader rotates around the X axis at the same rate. In addition, it also rotates around the Z axis for the Earth pointing. Now, according to the leader-follower formation control architecture, the followers are required to maintain their position as well as the attitude with respect to the leader. As mentioned in Section 3.1, a fixed formation configuration is assumed. Therefore, in this case the followers are required to maintain the same attitude as that of the leader relative to the inertial frame \mathcal{F}_0 .

For control and especially for diagnosis purpose, it is reasonable to utilize Euler angles. The reason for utilizing Euler angles is that attitude control performance specifications are usually available in terms of error in the Euler angles and the ground support personnel responsible for fault diagnosis are more comfortable dealing with Euler angles. Since the spacecraft attitude dynamics is specified in inertial

frame, PID controllers [135, 136] (with $\pm 5V$ limit or saturation for the control signal) are implemented for each axis of the leader based on “errors in terms of Euler angles” w.r.t. inertial frame obtained by performing the quaternion to Euler angle transformation (as discussed in Section 3.2). Followers’ PID controllers (with $\pm 5V$ limit or saturation for the control signal) have been designed based on “errors in term of the Euler angles” w.r.t. Leaders body-fixed frame obtained by performing the quaternion to Euler angle transformations.

3.2.2 Subsystem Component Model

In the model for synthetic data generation, the high fidelity mathematical model of the *Ithaco Type-A* reaction wheel that is available in [123] is utilized. As shown with a simplified schematic diagram in Figure 3.2, the model consists of detailed mathematical representation of a reaction wheel containing relationships to represent motor driver/torque control mechanism, motor disturbances such as cogging and ripple torques, Coulomb and viscous friction, torque noise that results due to lubricant dynamics, the “EMF torque limiting” phenomenon at high speed, safety mechanism for limiting speed, and torque bias discontinuity. Detailed discussion on the model and the reaction wheel parameter values are available in [123] and is not presented here. Under fault-free conditions, the reaction wheel is capable of delivering a maximum of $\pm 40\text{mN}\cdot\text{m}$ torque in response to a $\pm 5V$ torque command input voltage and operates within the speed range of $\pm 5100\text{rpm}$. For this research, the reaction wheel model has been modified to accommodate and support fault injection capabilities.

Ideal dynamics for attitude sensors are assumed; i.e., signals from sun sensors, horizon scanners, magnetometers, etc. have been assumed to be fed back to the attitude controller without any error or time delay.

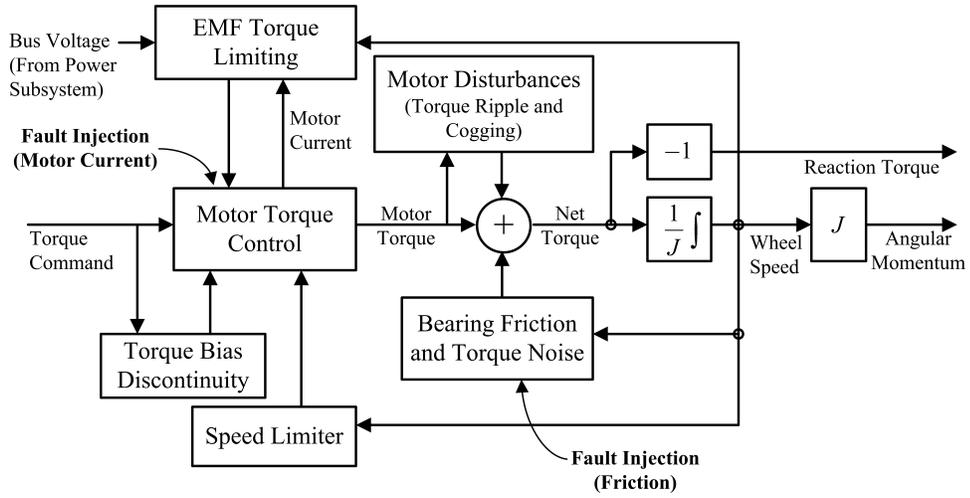


Figure 3.2: A simplified schematic diagram of a reaction wheel (adopted from [123]).

3.2.3 Environmental Disturbance Models

Satellites in a LEO orbit are subjected to different types of environmental disturbance torques such as magnetic, gravity gradient, aerodynamic, and solar radiation. The following disturbance models and parameters have been selected based on the information that is available in [137] and the mission specifications presented in Section 3.1.

Magnetic: The maximum magnetic torque that occurs in a polar orbit is given by: $T_{mag} = DB$; where D is the residual dipole of the spacecraft and B is the Earth magnetic field. B can be approximated as $B = \frac{2M}{R^3}$; where, M is the magnetic moment of the Earth ($M = 7.96 \times 10^{15} \text{ tesla}\cdot\text{m}^2$) and R is the radius of the orbit (in our case, $R = 6928 \times 10^3 \text{ m}$). Note that the magnetic torque is cyclic over the spacecraft orbit (as selected in Section 3.1) with peak value at the poles and half of the peak value at the equator. Consequently, the frequency of this cycle is twice that of the orbit. In this thesis the following is assumed, i.e.: $D = 0.8 \text{ A}\cdot\text{m}^2$ (*ampere-turn-m*²). Therefore, in this case, $T_{mag} = 3.83 \times 10^{-5} \text{ N}\cdot\text{m}$.

Gravity Gradient: The maximum gravity torque is given by: $T_{grg} = \frac{3\mu}{2R^3} |I_{xx} - I_{zz}| \sin(2\theta)$; where μ is the Earth's gravity constant ($3.986 \times 10^{14} \text{ m}^3/\text{sec}^2$), θ is the maximum deviation of x -axis (radial direction) from local vertical in *radians*, and I_{xx} and I_{zz} are the spacecraft inertia as provided in Section 3.1. In this thesis $\theta = 0.1 \text{ degree}$ is assumed. Therefore, in this case, $T_{grg} = 6.28 \times 10^{-9} \text{ N-m}$.

Aerodynamic: The maximum aerodynamic torque is given by: $T_{aero} = F(c_{pa} - c_g)$; where F is the force. F is approximated by $F = 0.5\rho C_d AV^2$; where c_{pa} is the center of aerodynamic pressure, c_g is the center of gravity, ρ is the atmospheric density, C_d is the drag coefficient (2 – 2.5), A is the surface area, and V is the spacecraft velocity. In the selected 550 km orbit, $V = 7585.2 \text{ m/s}$. In this thesis, the following values are assumed: $(c_{pa} - c_g) = 0.3 \text{ m}$, $\rho = 1.04 \times 10^{-13} \text{ kg/m}^3$, $C_d = 2.3$, $A = 1 \text{ m}^2$. Therefore, in this case, $T_{aero} = 2.06 \times 10^{-6} \text{ N-m}$.

3.3 Electrical Power Subsystem (EPS) Model

A simplified satellite electrical power subsystem (EPS) model has been incorporated, with the ACS model for each satellite. The EPS model [124], which is available in [125] and is developed in the virtual test bed (VTB) environment [124, 138], has been modified to incorporate fault injection capabilities and to ensure the supply of desired bus voltage to the ACS reaction wheels. A functional diagram of the EPS model of an individual satellite is shown in Figure 3.3, which consists of a solar array illumination model, solar array model, the controller or simplified power distribution and control unit (PDCU), a battery model, and a voltage regulator that delivers regulated bus voltage to the load; i.e., in our case, the reaction wheels.

It is important to mention that in the numerical simulations of the ACS, the pre-generated EPS bus voltage data that corresponds to the orbital characteristics (altitude, inclination, eclipse period, etc.) of the satellites are utilized. Therefore,

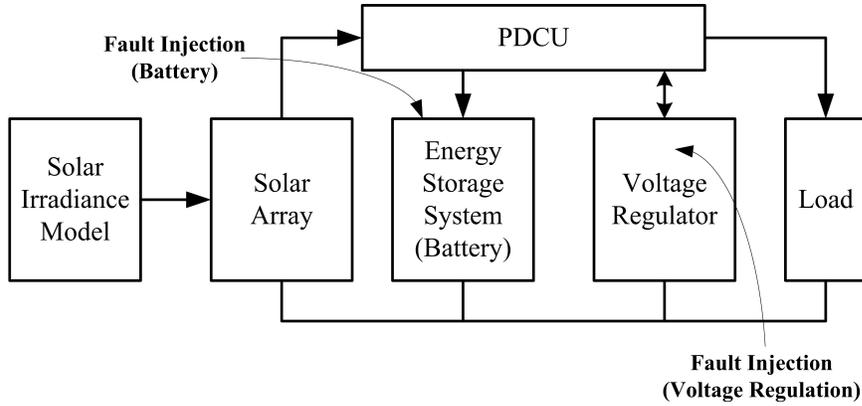


Figure 3.3: Functional diagram of the electrical power subsystem (EPS) (adopted from [124, 125]) depicting the locations of fault injections under the assumed EPS fault scenarios.

the interaction between the ACS and EPS is of the leader-follower type in the sense that any fault in the EPS may manifest in the ACS but the converse is not true. Such simulation setup is justified by the fact that the target ACS fault severities do not lead to excessively large deviations in the satellite attitude that may significantly affect the Sun pointing of the solar arrays, and hence the performance of the EPS.

3.4 Typical Simulation Results

In this section some sample simulations of the formation flight model that is utilized in this thesis are provided. Figure 3.4 shows the reference control signals to the ACS in quaternion over a 2-orbit period. Figures 3.4(b), 3.4(c), and 3.4(d) show the Euler angle representation of the reference signal where the angles corresponding to the X and the Z axes consist of some discontinuities. Figure 3.5 shows the actual attitude (in quaternion) of the leader satellite (Sat-1) and a follower satellite (Sat-3) relative to the inertial frame over an 2-orbit period. As mentioned in Section 3.2.1, the attitude control performance specifications are usually available in terms of error in the Euler angles and the ground support personnel responsible for fault diagnosis are more comfortable dealing with Euler angles.

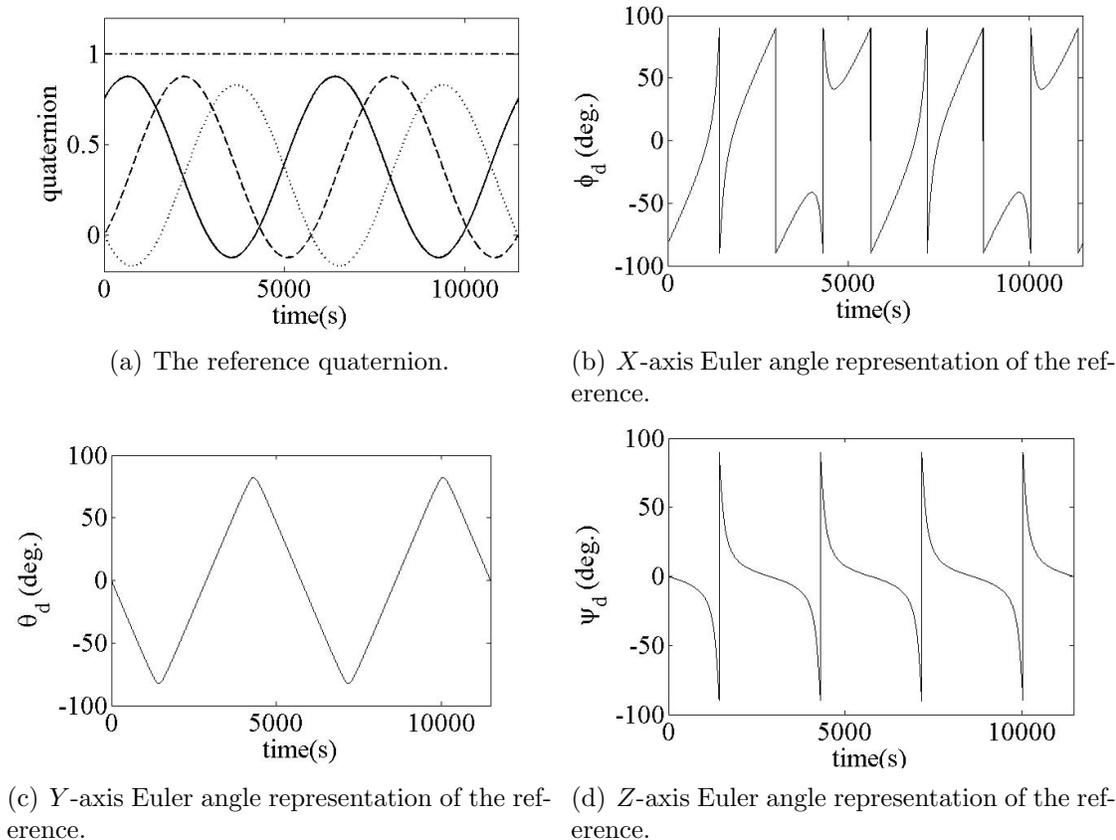


Figure 3.4: Reference attitude of the leader (Sat-1) relative to the inertial frame over 2-orbit period. In (a), the solid line represents q_1 , the dashed line represents q_2 , the dotted line represents q_3 , and the dashed-dotted line represents the constraint $\vec{q}^T \vec{q} + q_0^2 = 1$.

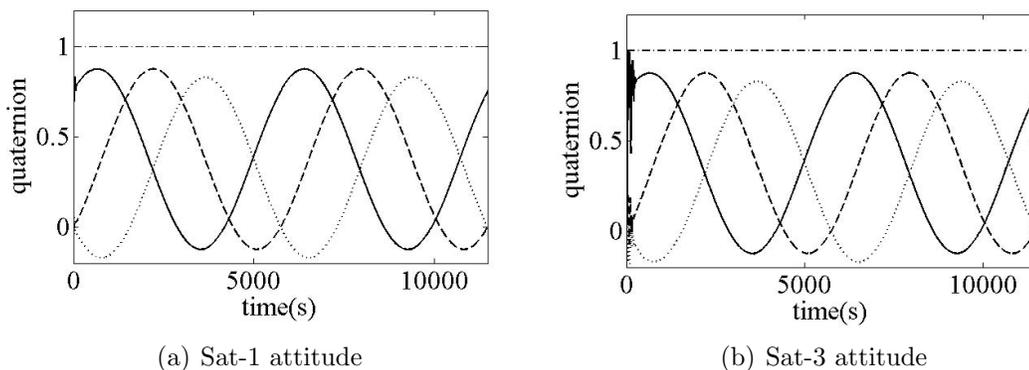


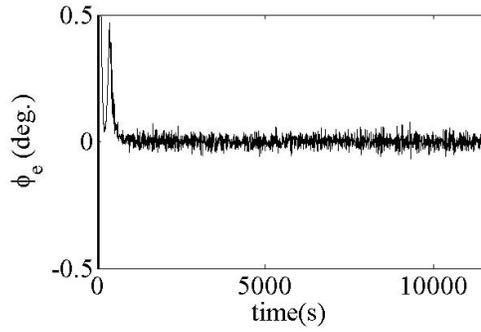
Figure 3.5: Attitude (in quaternion) of the leader (Sat-1) and a follower (Sat-3) relative to the inertial frame over 2-orbit period. The solid line represents q_1 , the dashed line represents q_2 , the dotted line represents q_3 , and the dashed-dotted line represents the constraint $\vec{q}^T \vec{q} + q_0^2 = 1$.

Figure 3.6 shows the attitude error (in Euler angles) of the leader (Sat-1) and a follower (Sat-3) in the inertial frame over 2-orbit period in terms of Euler angles with respect to the inertial frame \mathcal{F}_0 . The implemented 3-axis active PID control with reaction wheels provides RMS accuracy (1-sigma) [139] within 0.03 degree for the leader and 0.06 degree for the followers near zero reaction wheel speed over half-orbit period in steady state.

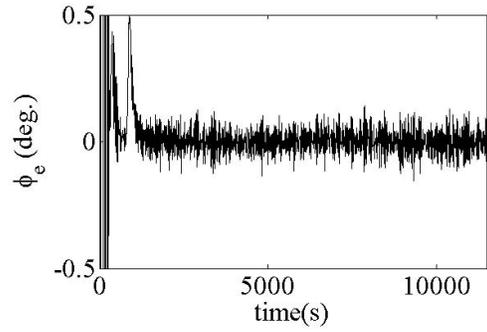
Figure 3.7 shows the relative attitude (in Euler angles) of a follower satellite (Sat-3) with respect to the leader (Sat-1), as well as with respect to another follower satellite (Sat-4) over a 2-orbit period. Note that in the simulated formation flight system the leader maintains a pre-specified attitude with respect to the inertial frame, and all the followers maintain the same attitude as that of the leader in the leader's body-fixed frame. Consequently, the steady state relative attitude that is to be maintained by the satellites are the same; i.e., $[0, 0, 0]$. Figures 3.8, 3.9, 3.10, and 3.11 show the reaction wheel (RW) actuator motor current, the motor torque, the control (torque command voltage), and the wheel speed, respectively of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period. Figure 3.12 shows some selected Electrical Power Systems (EPS) variables of a follower (Sat-3). Similar responses are observed for the leader as well as the other follower satellites in the formation, and the responses are not shown here in order to avoid redundancy.

3.5 Fault Simulation and Synthetic Data Generation

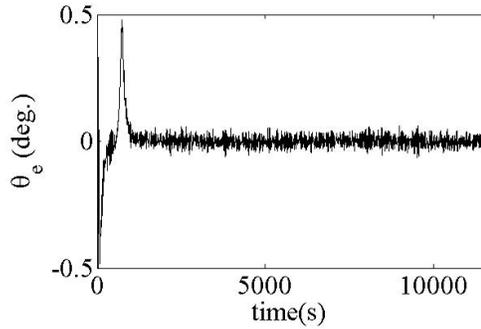
In this thesis, faults are injected when the formation flight is in steady state conditions (station-keeping mode) which implies that the orbital dynamics has negligible impact on the ACS fault diagnosis. Within the ACS, two types of intermittent faults are considered and are injected at the subsystem component (reaction wheel) level,



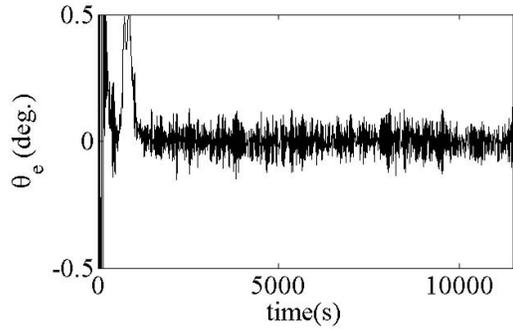
(a) Sat-1, error in the X -axis.



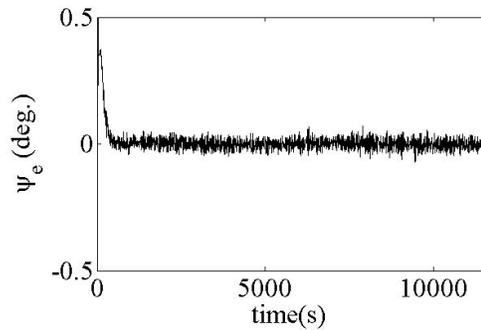
(b) Sat-3, error in the X -axis.



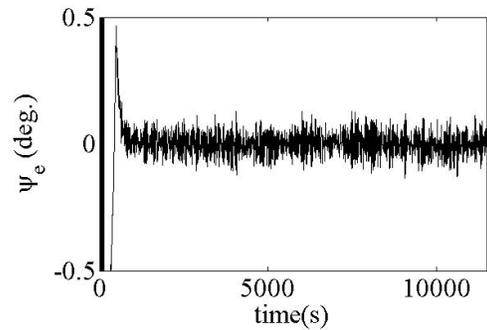
(c) Sat-1, error in the Y -axis.



(d) Sat-3, error in the Y -axis.

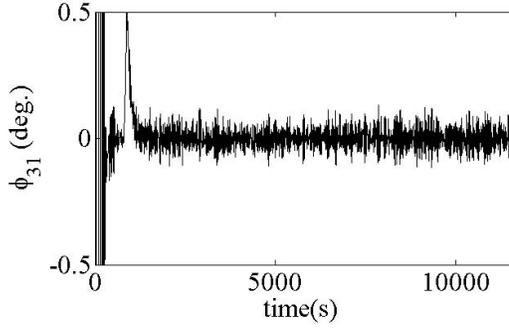


(e) Sat-1, error in the Z -axis.

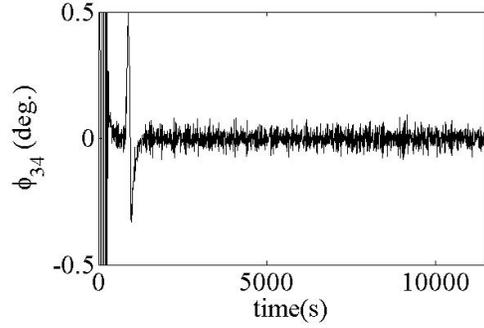


(f) Sat-3, error in the Z -axis.

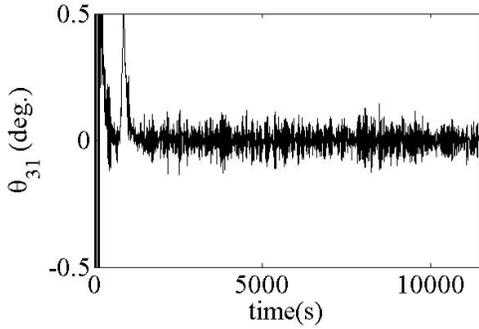
Figure 3.6: Attitude error (in Euler angles) of the leader (Sat-1) and a follower (Sat-3) in the inertial frame over a 2-orbit period.



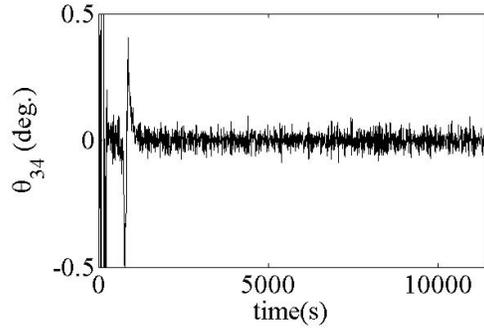
(a) Sat-3 attitude (X -axis) relative to Sat-1.



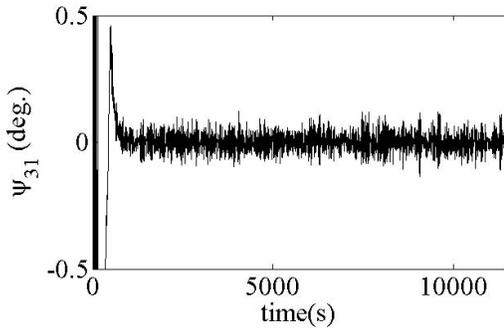
(b) Sat-3 attitude (X -axis) relative to Sat-4.



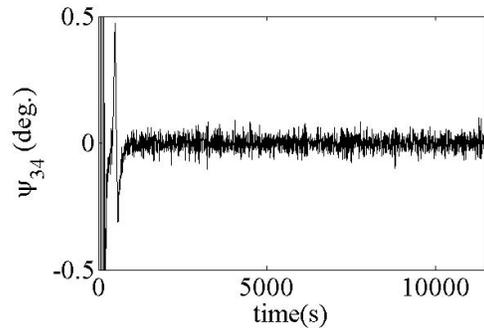
(c) Sat-3 attitude (Y -axis) relative to Sat-1.



(d) Sat-3 attitude (Y -axis) relative to Sat-4.



(e) Sat-3 attitude (Z -axis) relative to Sat-1.



(f) Sat-3 attitude (Z -axis) relative to Sat-4.

Figure 3.7: Relative attitude (in Euler angles) of one follower (Sat-3) with respect to the leader (Sat-1), and with respect to another follower (Sat-4) over a 2-orbit period.

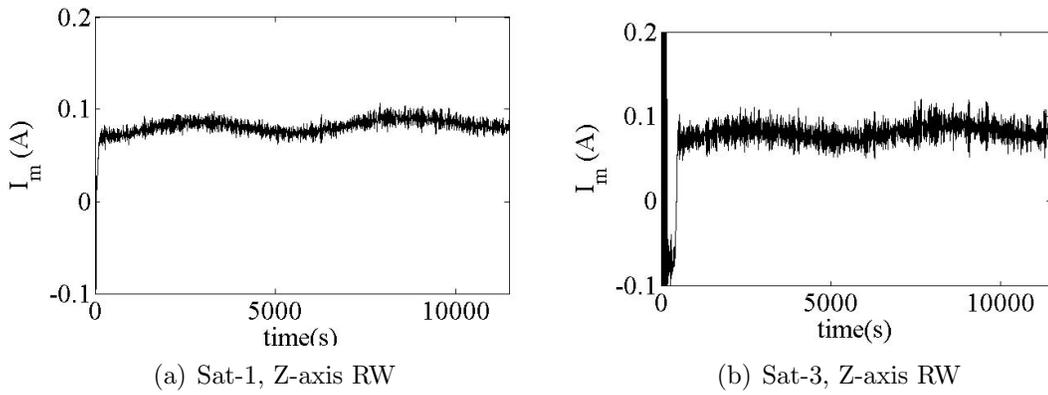


Figure 3.8: Reaction wheel (RW) motor current of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.

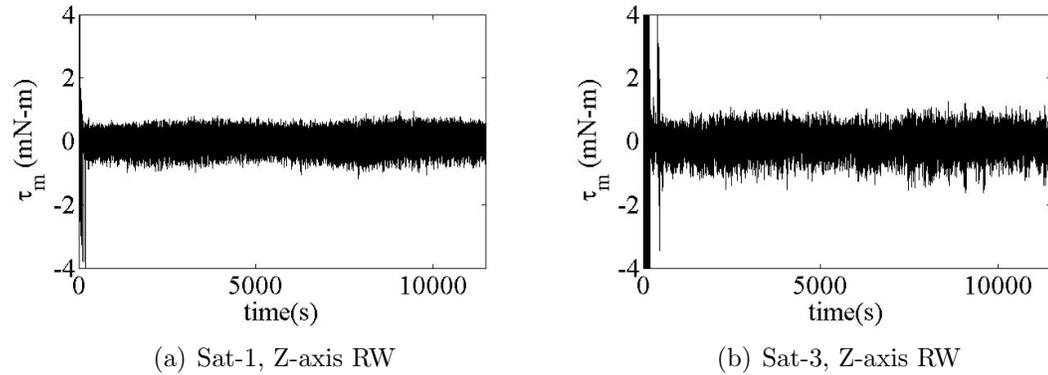


Figure 3.9: Reaction wheel (RW) motor torque of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.

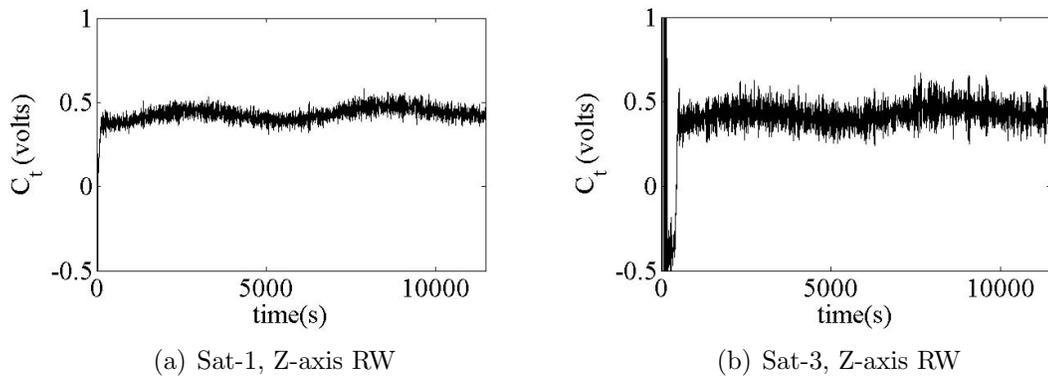
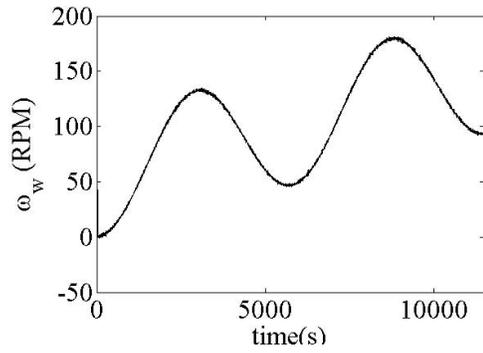
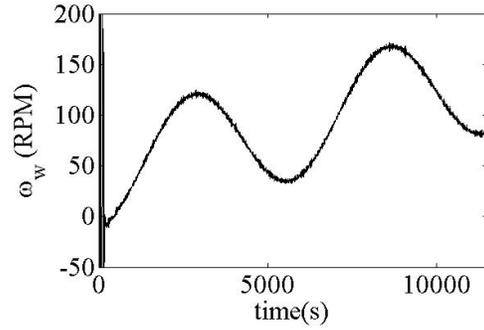


Figure 3.10: Reaction wheel (RW) control (torque command voltage) of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.

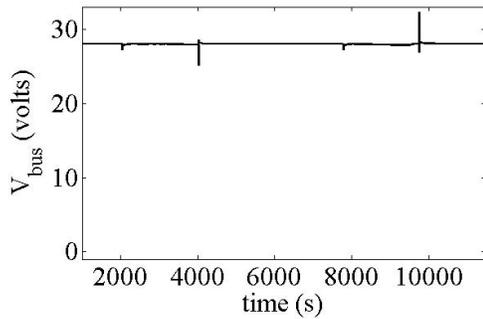


(a) Sat-1, Z-axis RW

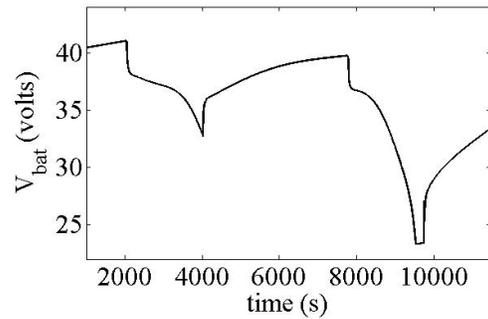


(b) Sat-3, Z-axis RW

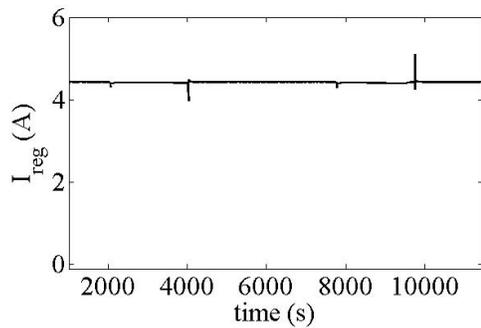
Figure 3.11: Reaction wheel (RW) speed of the leader (Sat-1) and a follower (Sat-3) over a 2-orbit period.



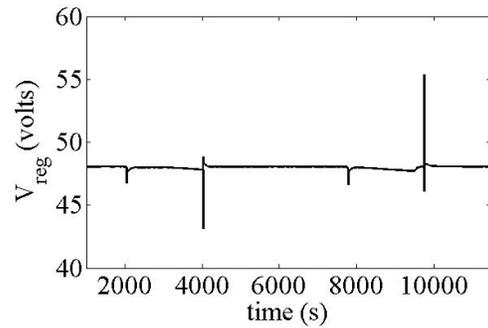
(a) Bus voltage.



(b) Battery voltage.



(c) Regulator output current.



(d) Regulator output voltage.

Figure 3.12: Selected electrical power systems (EPS) variables of a follower (Sat-3) under healthy condition.

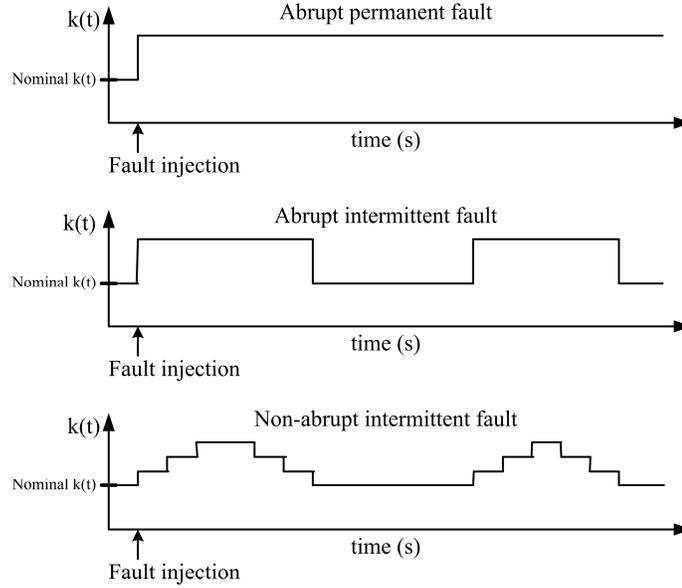


Figure 3.13: Changes of a component parameter $k(t)$ under different types of faults namely, abrupt permanent fault, abrupt intermittent fault, and non-abrupt intermittent fault.

namely: (a) friction fault (increase in the viscous friction), and (b) reaction wheel motor current fault (decrease in the motor gain). The reason behind considering these two faults is that anomalies in reaction wheels often lead to ACS failure in satellites [140]. The *friction fault* may occur due to the wear and tear of the wheel bearing material over time or due to some problems in the lubricant flow. The *motor current fault* may occur because of some electronic hardware malfunctions in the motor driver unit (MDU) of the reaction wheel.

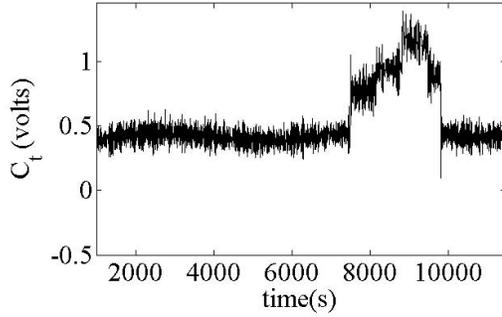
Each fault is injected with 3 (three) severity levels: gradually increasing from the lowest to the maximum severity and then gradually decreasing before a complete fault removal. Note that the faults are intermittent and non-abrupt in nature. Figure 3.13 shows the changes in a component parameter, denoted by $k(t)$, under different types of faults, where after fault injection $k(t)$ deviates from its nominal value differently under each type of a fault. The fault injection locations in the ACS reaction wheels are shown in Figure 3.2. For all the reaction wheel faults discussed above the attitude accuracy decreases: the pointing accuracy measure (1-sigma)

decreases beyond the assumed specification; i.e., 0.03 degree for the leader and 0.06 degree for the followers as mentioned in Section 3.2.1.

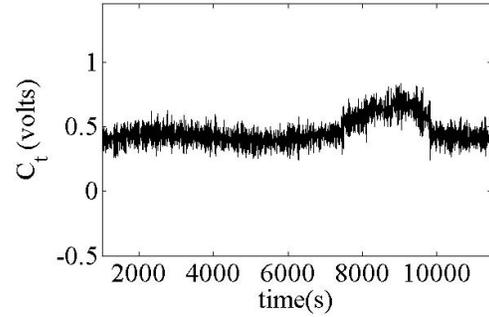
Figure 3.14 shows the Z -axis reaction wheel (RW) torque command voltages (C_t), motor currents (I_m) and wheel speeds (ω_w) of a follower (Sat-3) in the presence of a motor current fault and a friction fault that are injected in the Z -axis reaction wheel of Sat-3 between $t = 7500$ s and $t = 9810$ s. Note that the nominal behaviors are presented in Figures 3.8, 3.9, 3.10, and 3.11. Figure 3.15 shows the X and Y axes reaction wheel (RW) torque command voltages (C_t), motor currents (I_m) and wheel speeds (ω_w) of a follower (Sat-3) in the presence of a motor current fault and a friction fault that are injected in the Z -axis reaction wheel of Sat-3 between $t = 7500$ s and $t = 9810$ s. It is observed from this figure that the motor current fault in the Z -axis RW does not manifest in the RWs in the X and Y axes. Similar observation was made for the friction fault which is not shown here in order to avoid redundancy.

Figure 3.16 shows the fault manifestations in the relative attitude (in Euler angles) of one follower (Sat-3) with respect to the leader (Sat-1), and with respect to another follower (Sat-4) when a motor current fault is injected between $t = 7500$ s and $t = 9810$ s in the Z -axis reaction wheel of Sat-3.

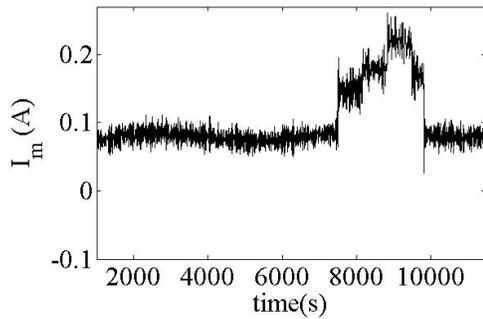
Within the EPS, two types of faults are considered at the subsystem level, namely: (a) an intermittent bus voltage drop due to the voltage regulator malfunctioning, and (b) an intermittent bus voltage drop due to anomaly in the battery. Each fault is injected by introducing undesired resistances at the battery output and voltage regulator output, respectively (fault injection locations are shown in Figure 3.3) with 3 (three) severity levels: gradually increasing from the lowest to the maximum severity and then gradually decreasing before a complete fault removal. Therefore, the faults are intermittent and non-abrupt in nature. Note that although



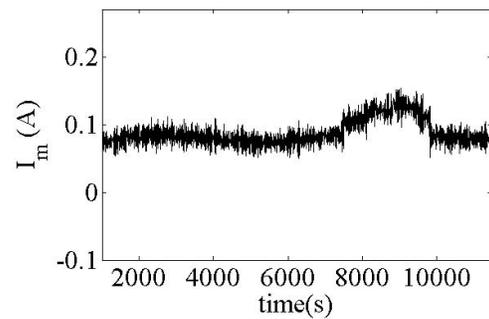
(a) Sat-3, C_t under current fault.



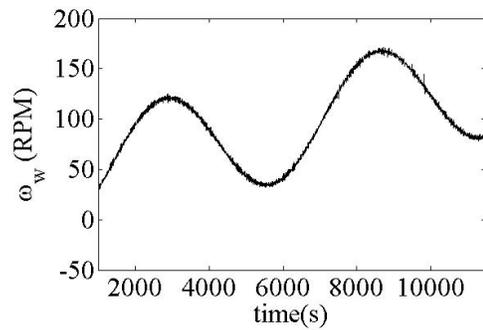
(b) Sat-3, C_t under friction fault.



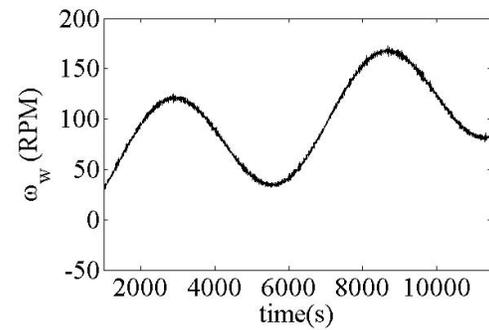
(c) Sat-3, I_m under current fault.



(d) Sat-3, I_m under friction fault.



(e) Sat-3, ω_w under current fault.



(f) Sat-3, ω_w under friction fault.

Figure 3.14: The Z -axis reaction wheel (RW) torque command voltages (C_t), motor currents (I_m) and wheel speeds (ω_w) of a follower (Sat-3) in the presence of a motor current fault and a friction fault in the Z -axis reaction wheel of Sat-3 (both faults injected between $t = 7500$ s and $t = 9810$ s).

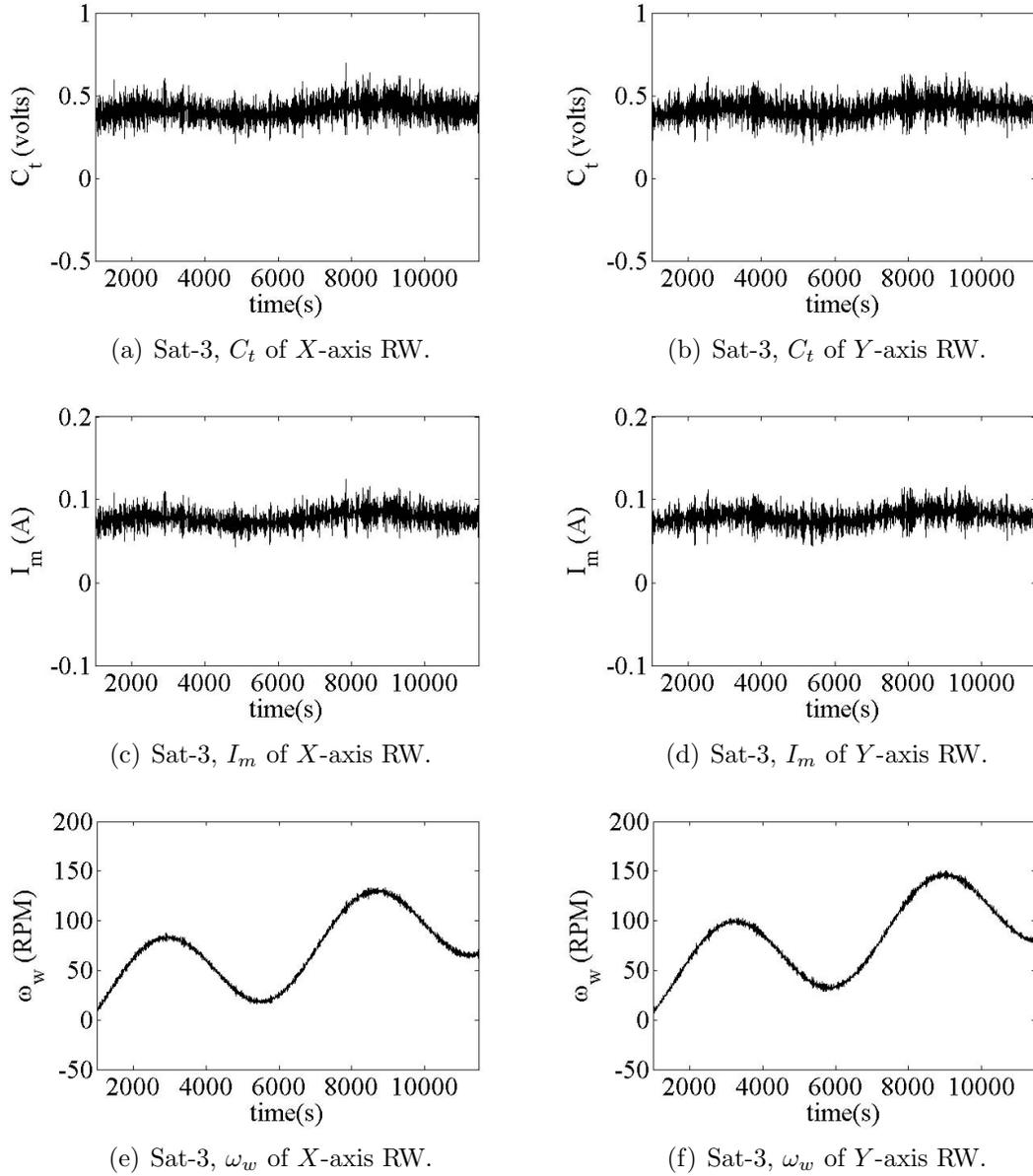
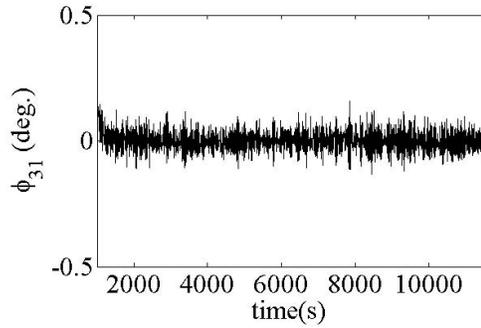
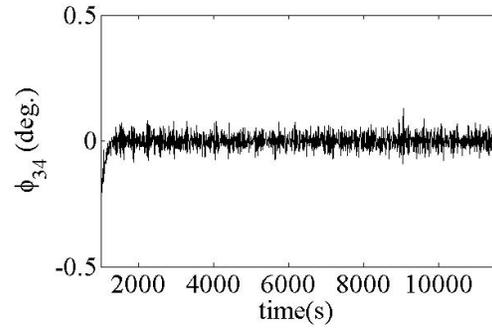


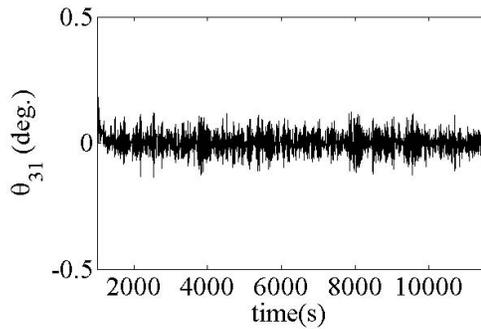
Figure 3.15: The X and Y axes reaction wheel (RW) torque command voltages (C_t), motor currents (I_m) and wheel speeds (ω_w) of a follower (Sat-3) in the presence of a motor current fault in the Z-axis reaction wheel of Sat-3 (injected between $t = 7500$ s and $t = 9810$ s).



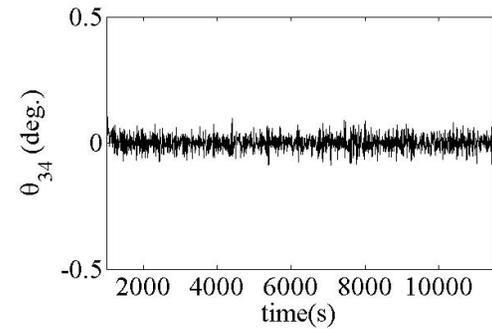
(a) Sat-3 attitude (X -axis) relative to Sat-1.



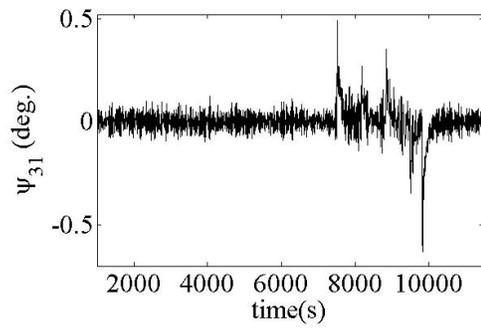
(b) Sat-3 attitude (X -axis) relative to Sat-4.



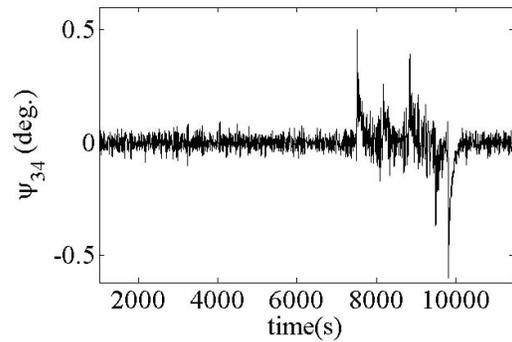
(c) Sat-3 attitude (Y -axis) relative to Sat-1.



(d) Sat-3 attitude (Y -axis) relative to Sat-4.



(e) Sat-3 attitude (Z -axis) relative to Sat-1.



(f) Sat-3 attitude (Z -axis) relative to Sat-4.

Figure 3.16: Relative attitude (in Euler angles) of one follower (Sat-3) with respect to the leader (Sat-1), and with respect to another follower (Sat-4) in the presence of a motor current fault in the Z -axis reaction wheel of Sat-3 (injected between $t = 7500$ s and $t = 9810$ s).

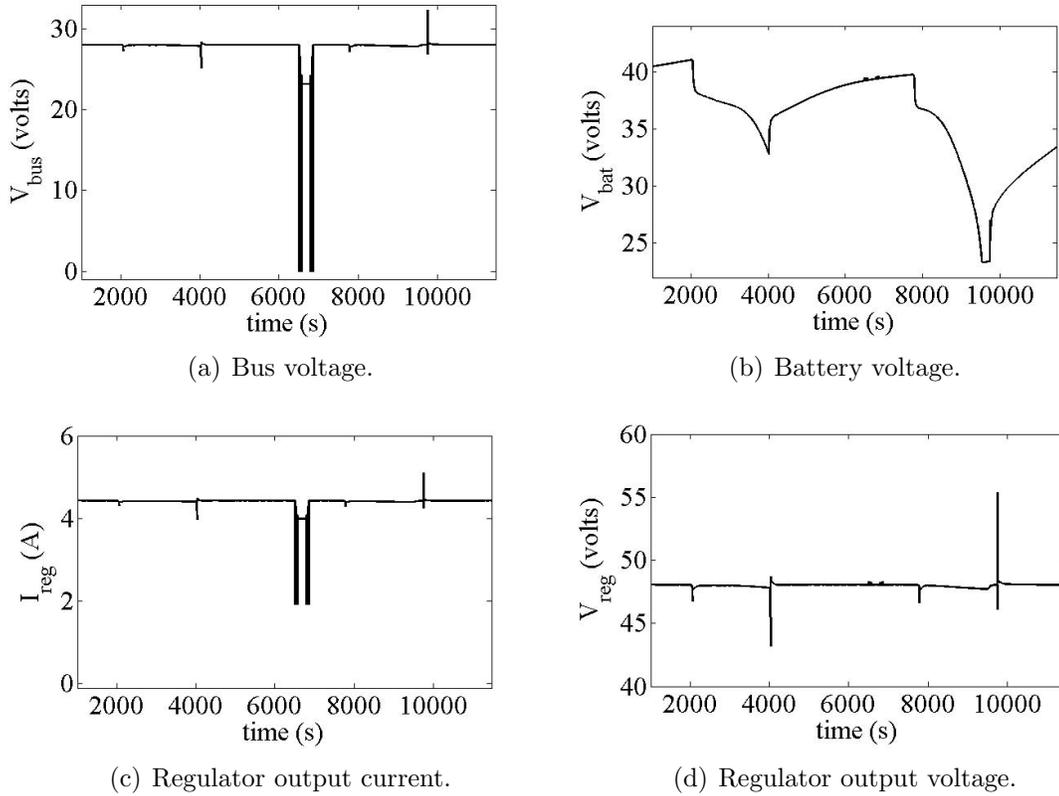


Figure 3.17: Selected electrical power subsystem (EPS) variables of a follower (Sat-3) under a regulator fault (injected between $t = 6500$ s and $t = 6860$ s).

component level faults are being considered within the ACS, the faults corresponding to the EPS are at the subsystem level due to the lack of detailed understanding and a prior knowledge of the EPS components within the EPS. Consequently, the EPS fault diagnosis is performed only up to the subsystem level (the different levels, namely component, subsystem, system, and formation will be defined formally in Section 4.1).

Figure 3.17 shows some selected electrical power subsystem (EPS) variables of a follower (Sat-3) under a regulator fault that is injected between $t = 6500$ s and $t = 6860$ s. Note that the fault causes the bus voltage to drop during the entire fault injection period.

Figure 3.18 shows the same selected electrical power subsystem (EPS) variables of a follower (Sat-3) under a battery fault that is injected between $t = 6500$ s and

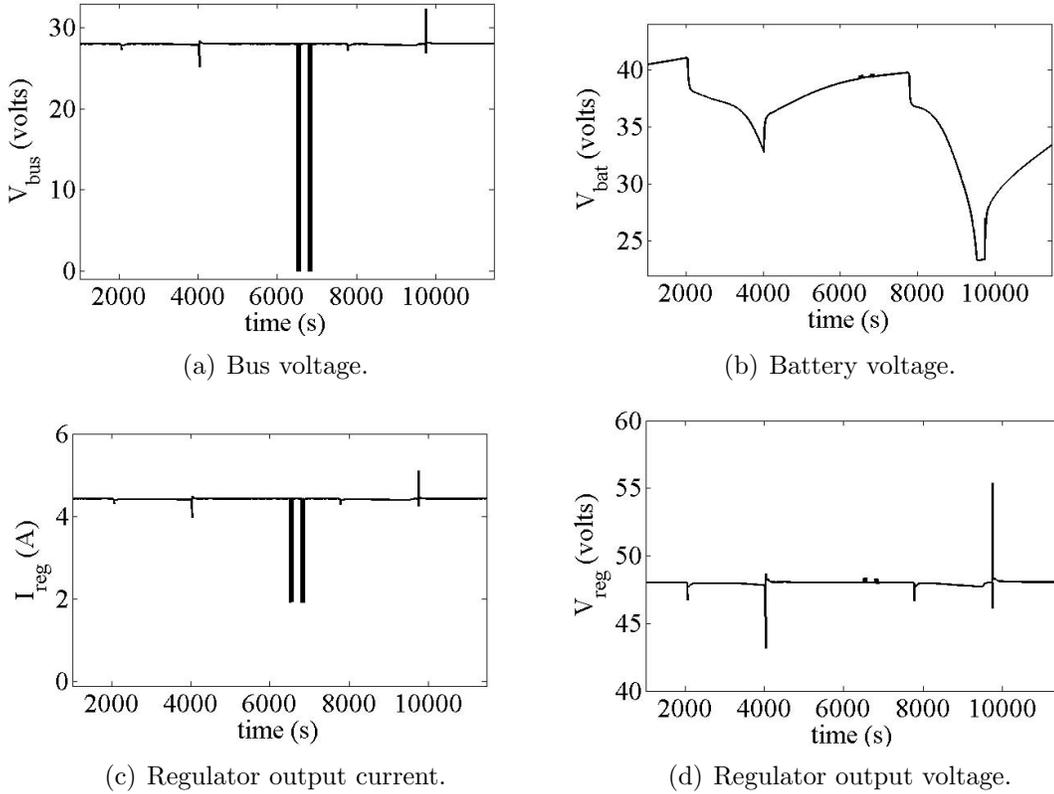


Figure 3.18: Selected electrical power subsystem (EPS) variables of a follower (Sat-3) under a battery fault (injected between $t = 6500$ s and $t = 6860$ s).

$t = 6860$ s. Note that unlike the regulator fault, the battery fault does not cause the bus voltage to drop during the entire fault injection period.

3.6 Summary

In this chapter, the model that was implemented in this thesis for generating synthetic formation flight data is presented. Detailed descriptions of the two satellite subsystems, namely the attitude control subsystem (ACS) and the electrical power subsystem (EPS) are provided. Some typical simulation data for the two subsystems as well as some relative attitude data of the satellites in a formation flight are presented under both healthy and faulty conditions of the space platform. The

utilization of synthetic formation flying system data was necessary due to the unavailability of actual telemetry data from an actual and real operational formation flight space mission.

Chapter 4

Hierarchical Fault Diagnosis Framework

In this chapter first a hierarchical fault diagnosis framework that is proposed in this thesis for ground-based formation flight health monitoring and fault diagnosis is presented. Next, a generic fault diagnosis model is discussed which is utilized throughout the thesis.

4.1 Development of a Hierarchical Fault Diagnosis Framework

The proposed fault diagnosis strategy aims to perform diagnostic reasoning in complex systems such as a “formation flight system” by decomposing its complex structure hierarchically into simpler modules or components. The decomposition is driven by the need, from project management perspective, for supporting the development of the components/subsystems of the overall system by a number of teams and performing integration at the end. Though the proposed framework is generic in nature and includes various spacecraft subsystems, in this thesis the discussion is mostly

confined within the attitude and orbital control subsystem and electrical power subsystem. Furthermore, the availability of some fault detection mechanisms at each level in the hierarchy is assumed and the proposed framework is discussed mostly from fault diagnosis or isolation perspective.

Figure 4.1 shows the proposed 4-layer hierarchical decomposition from the perspective of the attitude and orbital control of the satellites in a formation flight. In Figure 4.1, fault diagnosis at level 1 (subsystem component level) corresponds to

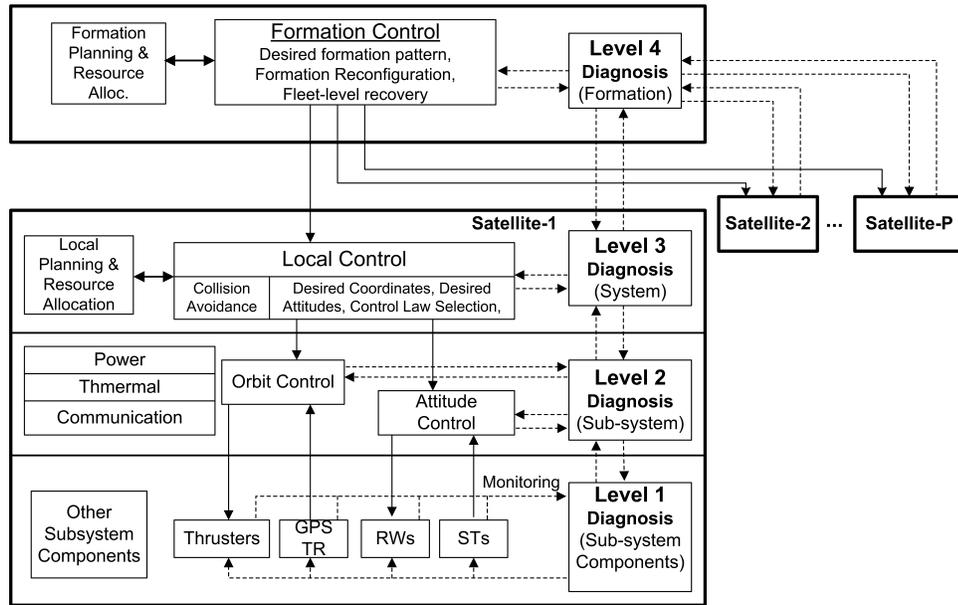


Figure 4.1: Proposed fault diagnosis framework for a multi-platform space system.

sensor and actuator fault diagnosis. Note that often it is not necessary to identify fault causes beyond this level because recovery actions or redundancies are not applied within these components. In the case of the attitude and orbital control subsystem (AOCS), reaction wheels, thrusters, earth-sensors, star trackers, relative position and attitude sensors, etc. are the components. It is important to note that as pointed out in [141], the runtime contingencies in spacecraft are usually the hardware/subsystem component failures (though it is also possible to have flaws in planning, and to have unexpected outcomes in execution).

Fault diagnosis at level 2 (subsystem level) corresponds to different subsystems

such as attitude, orbital, power, etc. Fault diagnosis is performed for different subsystems by utilizing the health state information available from different subsystem components. However, strict partitioning of FDI for different subsystems may not be possible in many cases because spacecraft operation is characterized by concurrent activities across a relatively large number of different subsystems [141, 142].

Level 3 (system level) diagnosis is performed by utilizing the health state information available from different subsystems (for example, attitude control subsystem (ACS), thermal subsystem, power subsystem, etc.), their interactions and expected behaviors/behavior specifications. In level 4 (formation level) diagnosis, individual spacecraft in the formation are considered as different “components” of the formation flying system. This level is unique to multi-platform missions. Therefore, at this level fault detection refers to a decision making about the existence of an anomaly in the formation components, i.e., in one or more satellites in the formation. The objective of fault diagnosis or isolation is to identify particular spacecraft that are faulty. Note that the system level diagnosis in a specific spacecraft does not consider the existence of other spacecraft in the formation.

4.2 Level l Fault

First, we take into consideration that even if a fault is originated in a subsystem component, the fault is assumed to have different levels of manifestations in the hierarchy. In other words, for performing diagnosis at different levels, it is assumed that fault symptoms/manifestations are available. As an example, consider the specific fault of “increase in friction” in the pitch reaction wheel (subsystem component). At the subsystem component level, one of the fault manifestations would be “high current drawn by the wheel motor”. In the attitude control subsystem (ACS) level,

one of its manifestations would be “deviation from expected pitch angle”. The system level manifestations can be described in terms of deviations of the ACS behavior specifications relative to other subsystems. Finally, at the formation level the most important fault manifestations will be “deviation from expected relative attitude with respect to other satellites”. This is because the main purpose of formation flying is to form a virtual structure such as a telescope in space for which precision control of the relative positions and attitudes of the satellites are a requirement.

Therefore, there is a need for identifying faults differently at various levels in the hierarchy based on the “level of abstraction” at a particular level and the manifestation of a fault at that particular level. On the other hand, in the case of a system level anomaly that leads to a situation in which a wrong command is sent to the actuator, the subsystem component, or even the subsystem, would follow the “wrong” command without being aware of the anomaly. Based on the above observations, the definition of an “level l fault” [143] is formally stated as follows:

Definition 4.2.1 (Level l Fault [143]). A fault occurring in a system that is hierarchically decomposed into L levels is said to be an “level l fault” ($l = 1, 2, \dots, L$) and is denoted by fault f_k^l (k -th fault mode) if and only if its manifestations are only observable in the fault signatures that belong to level l and in higher levels for the fault severity level(s) under consideration.

In Definition 4.2.1, the term “observable” is not associated with the notion of “observability” that is used in control theory. In this thesis, features that are extracted from process states and/or variables are utilized as *diagnostic signals*. A *fault manifestation* corresponding to a specific fault is considered to be some pre-identified value(s) of a diagnostic signal that indicates the presence of that fault. The *fault signature* is represented in the form of rule(s) that identifies all the fault manifestations of interest for that specific fault (discussed in detail in Chapter 5).

Distinguishing faults at different levels based on the above definition would

allow one to avoid cycles in a directed graph-based diagnostic reasoning model; i.e., by utilizing the concept of different levels of fault one can develop an acyclic directed graph model for diagnosis.

4.3 Generic Directed Graph Representation

The proposed hierarchical decomposition, shown in Figure 4.1, is represented with a generic directed acyclic graph as shown in Figure 4.2. The entire system under consideration is represented with a single node at the highest level that consists of subcomponents located at the lower levels. A directed arc between two components represents the influence of the health state of one component on that of another. The p -th component at level l in the hierarchy is denoted as C_p^l . For example, in the

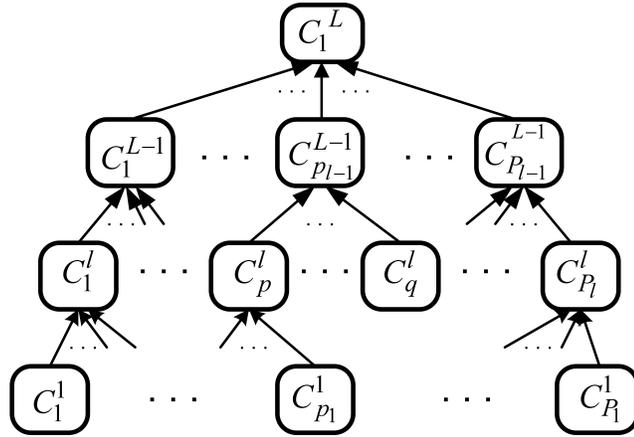


Figure 4.2: Directed graph representation of the proposed hierarchical fault diagnosis.

case of a multi-platform space system, for $l = 1$, C_p^1 would correspond to a sensor or an actuator whereas for $l = L$, C_1^L would correspond to the “satellite formation component”. Let the set of all components located in two levels, namely l_1 and l_2 , in the proposed hierarchical organization be denoted as $C_p^{l_1}$ and $C_q^{l_2}$, respectively; where $p = 1, 2, \dots, P_{l_1}$; $q = 1, 2, \dots, Q_{l_2}$; $l_1, l_2 \in \{1, 2, \dots, L\}$; with L denoting the total number of hierarchy levels. Therefore, when $l_1 = l_2 = l$, two different components

located at the same level l are represented as C_p^l and C_q^l , assuming $P_l = Q_l$ as shown in Figure 4.2. For any C_p^l , the sets of components that are parents of C_p^l are denoted by $pa(C_p^l)$. A node C_p^l is a leaf node if $pa(C_p^l) = \emptyset$. Based on this generic directed graph representation the problem of fault diagnosis is divided into two stages:

First, fault diagnosis schemes for identifying faults at different nodes of Figure 4.2 are developed. In Chapter 5, a hierarchical fault diagnosis model (HFDM) is developed. In the proposed HFDM, fuzzy rule-based reasoning is employed to identify the health states at different nodes, and a hierarchical diagnosis algorithm is proposed for identifying the origin of the fault. Fuzzy rules are developed for fault diagnosis at different levels in the hierarchy by taking into account the uncertainties in the fault manifestations in a given component. However, in this model the component interaction are quantified without taking the uncertainties in the component health state dependencies into account. This may be realistic in many practical situations. In the second stage, this limitation is overcome by developing a component dependency model (CDM) which is discussed next in the subsequent paragraph.

In Chapter 6, a Bayesian network-based component dependency model (CDM) is developed. In the model, component dependencies are quantified by the conditional probability distributions that are associated with the CDM nodes. Note that at a given node fuzzy rule-based diagnosis is still applied although the CDM is flexible to accommodate other fault diagnosis methodologies at different nodes. Furthermore, although the development of the proposed methodology is based on the health management of satellites formation flight, the methodology is generic enough to be applicable to other systems or a fleet of systems that require health monitoring decision support systems (DSS).

4.4 Fault Propagation

When a fault is detected in a system, the objective of diagnosis is to identify its cause or location. When diagnosis is not hierarchical and performed only for one specific component or system, the standard way to evaluate performance is to construct a confusion matrix and compute accuracy, misclassification rate, etc. The diagnosis of a single component corresponds to the diagnosis at a node of the proposed directed graph model shown in Figure 4.2. However, in hierarchical diagnosis fault identifications at different nodes are required to be related in order to determine the propagation and the node where the fault originated.

Now consider a general scenario where in the directed graph-based representation a faulty state of a node C_p^l is detected and identified, and the node is located at an intermediate level; i.e., $1 < l < L$. If $pa(C_p^l) \neq \emptyset$, the fault did not originate at that node. Therefore, the objective of diagnosis translates to the identification of the node where the fault originated. Furthermore, it is of interest to identify the components that are affected by the fault. A fault propagation path identifies the origin of a fault and all the components that are affected by the fault.

Let $C_{p_2}^{l_2}$ be the node at an intermediate level l_2 with some identified faulty state $X_{p_2}^{l_2} = \bar{x}_0$. Let $C_{p_1}^{l_1}$ be a leaf node ($pa(C_{p_1}^{l_1}) = \emptyset$) where the fault has originated. Further, let $\pi(C_{p_2}^{l_2})$ and $\sigma(C_{p_2}^{l_2})$ denote the sets of predecessors and successors of node $C_{p_2}^{l_2}$, respectively in the CDM (or HFDM). Therefore, $C_{p_1}^{l_1} \in \pi(C_{p_2}^{l_2})$; where $l_2 > l_1$. A candidate (possible) fault propagation path is defined as follows.

Definition 4.4.1 (Candidate Fault Propagation Path). A candidate fault propagation path is a directed path that identifies all the affected components associated with a fault at a node $C_{p_2}^{l_2}$, and the i -th candidate fault propagation path is denoted as $path_i(C_{p_2}^{l_2}) = C_{p_1}^{l_1} \rightarrow \dots C_{q_1}^{l_2-1} \rightarrow C_{p_2}^{l_2} \rightarrow C_{q_2}^{l_2+1} \rightarrow \dots C_{p_3}^{l_3}$.

A path $path_i$ is said to be a *fully identified fault propagation path* if and only

if $\forall C_p^l \in path_i$, faults have been identified. If faults are identified only at some of the nodes in the $path_i$, the path is said to be a *partially identified fault propagation path*. Note that the nodes in the path segment $C_{p_1}^{l_1} \rightarrow \dots C_{q_1}^{l_2-1}$ belong to $\pi(C_{p_2}^{l_2})$, and the nodes in $C_{q_2}^{l_2+1} \rightarrow \dots C_{p_3}^{l_3}$ belong to $\sigma(C_{p_2}^{l_2})$. The set of all such candidate fault propagation paths associated with the identified faulty state of $C_{p_2}^{l_2}$ is denoted as $PATH(C_{p_2}^{l_2})$.

4.5 Summary

In this chapter, a fault diagnosis framework for a multi-platform space system is developed. The concept of level l fault is introduced and formally defined. Next, a generic directed graph-based fault diagnosis model is presented which will be utilized in the next two chapters of the thesis. Finally, the identification of the fault propagation in a hierarchically decomposed system is discussed. In the next chapter, fuzzy rule-based fault diagnosis is investigated for multi-platform space systems.

Chapter 5

Fuzzy Rule-Based Fault Diagnosis

In this chapter fuzzy rule-based fault diagnosis is investigated at different levels of the proposed hierarchical decomposition that was presented in Chapter 4.

5.1 Introduction

In Chapter 4, the proposed hierarchical framework for multi-platform space systems and specifically for satellites formation flight fault diagnosis was discussed in detail. The proposed hierarchical fault diagnosis was represented by a generic directed graph model. In this chapter, the framework and the associated generic directed graph model is formalized in terms of fuzzy rule-based reasoning. Fuzzy rule-based reasoning is investigated because of its well-known ability for accommodating uncertainties in fault symptoms, and performing diagnosis by utilizing rules that are transparent to human operators or users. As discussed in Section 1.3, when the system or the application domain is very large, rule-based representation of the entire system leads to a large and inefficient knowledge base, causing a poor quality in diagnosis. However, in this thesis we decompose the system under consideration into multiple levels and components. Such decomposition allows the use of fuzzy rule-based reasoning separately in the components of a large and complex system

such as a formation flight system. The organization of this chapter is as follows: In Section 5.2 the proposed hierarchical fault diagnosis framework is formalized and a fuzzy rule-based fault diagnosis methodology within the proposed framework is presented. In Section 5.3, the proposed scheme is demonstrated by using synthetic data from the formation flight system model that was presented in Chapter 3. The performance evaluation results are presented in Section 5.4, and advantages as well as the limitations of the scheme are discussed in Section 5.5. Finally, the chapter is summarized in Section 5.6.

5.2 Development of a Hierarchical Fault Diagnosis Model (HFDM)

This section is divided into five parts: In Section 5.2.1, the proposed hierarchical structure is formally presented and the key terminologies and definitions that are necessary for the proposed scheme are presented. The properties of the proposed hierarchical structure are stated in Section 5.2.2. In Sections 5.2.3 and 5.2.4, fuzzy rule-based fault diagnosis is investigated for independent and dependent components (as defined in Section 5.2.1), respectively. A hierarchical fault diagnosis algorithm is presented in Section 5.2.5.

5.2.1 HFDM Structure, Terminologies and Basic Definitions

The proposed hierarchical decomposition is represented with a generic directed acyclic graph structure as shown in Figure 5.1 where the entire system under consideration is represented with a single node at the highest level that consists of subcomponents located at the lower levels. In this chapter, we identify this structure as a hierarchical fault diagnosis model (HFDM). We denote the p -th component at level l in the hierarchy as C_p^l . For example, in the case of a multi-platform space

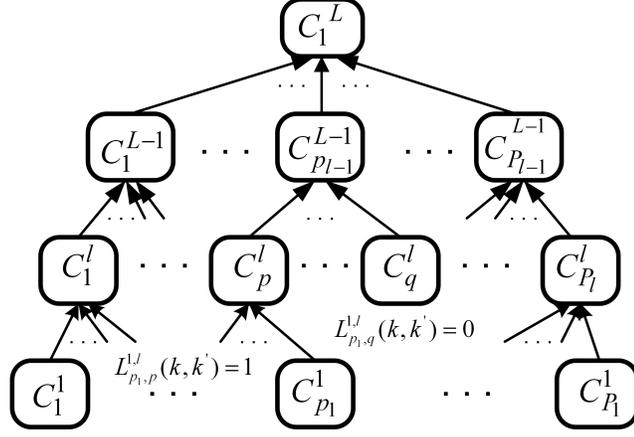


Figure 5.1: Directed graph representation of the proposed hierarchical fault diagnosis model (HFDM).

system, for $l = 1$, C_p^1 would correspond to a sensor or an actuator whereas for $l = L$, C_1^L would correspond to the “satellite formation component”. Let the set of all components located in two levels namely, l_1 and l_2 , in the proposed hierarchical organization be denoted as $C_p^{l_1}$ and $C_q^{l_2}$, respectively; where $p = 1, 2, \dots, P_{l_1}$; $q = 1, 2, \dots, Q_{l_2}$; $l_1, l_2 \in \{1, 2, \dots, L\}$; with L denoting the total number of hierarchy levels. Therefore, when $l_1 = l_2 = l$, two different components located at the same level l are represented as C_p^l and C_q^l , assuming $P_l = Q_l$ as shown in Figure 5.1. For any C_p^l , the sets of components that are parents of C_p^l (as represented in Figure 5.1) are denoted by $pa(C_p^l)$.

For fault diagnosis/isolation of physical systems, relationships among observed symptoms and faults are necessary. Symptoms are the manifestations of the faults in the available diagnostic signals (measured from the process or analytically calculated). In other words, symptoms are obtained by monitoring some pre-identified diagnostic signals that are of one of the following types [19]: (1) residuals that are generated based on the system models, (2) binary or multi-valued signals that are resulting from residual classification/quantification, (3) statistical parameters or features that are describing signal properties, and (4) process states and/or variables (measured or calculated).

In this thesis, we utilize features that are extracted from process states and/or variables as *diagnostic signals*. Furthermore, a *fault manifestation* corresponding to a specific fault in this thesis is considered to be some pre-identified value(s) of a diagnostic signal that indicates the presence of that fault. The *fault signature* is represented in the form of rule(s) that identifies all the fault manifestations of interest for that specific fault. A *fault signature model* of a component refers to a set of rules that corresponds to all the faults that are to be identified in that component. Diagnostic signals, fault manifestations, and fault signatures are formally specified in Section 5.2.3.

The set of P_l components located at level l is denoted as C^l . The components, manifestable faults, diagnostic signals, fault manifestations, and fault signature models of the p -th component at level l are denoted by C_p^l , F_p^l , S_p^l , M_p^l , and FSM_p^l , respectively; where $p = 1, 2, \dots, P_l$. The fault signature model (FSM_p^l) of C_p^l consists of fault signatures that correspond to both types of faults — the ones that are originated at C_p^l and the ones that are originated at some lower level but manifested at C_p^l . It should be noted here that if $pa(C_p^l) \neq \emptyset$, a fault $f_k^l \in F_p^l$ and its corresponding fault signature in FSM_p^l may represent more than one fault that originates at some lower levels which will be formally stated in Proposition 5.2.2 in Section 5.2.4.

We distinguish the components within the proposed hierarchical decomposition according to the following definitions:

Definition 5.2.1 (Independent Component). For any given fault severity level under consideration, a component $C_p^{l_1}$ is independent of another component $C_q^{l_2}$, where $l_1 > l_2$, if a change in the diagnostic signal value(s) in $C_q^{l_2}$ never manifests or leads to a change in the diagnostic signal value(s) in $C_p^{l_1}$ due to the presence of any fault $f_k^{l_3}$; where $l_2 \geq l_3$.

Definition 5.2.2 (Dependent Component). For any given fault severity level

under consideration, a component $C_p^{l_1}$ is dependent on another component $C_q^{l_2}$, where $l_1 > l_2$, if a change in the diagnostic signal value(s) in $C_q^{l_2}$ always manifests or leads to a change in the diagnostic signal value(s) in $C_p^{l_1}$ due to the presence of some fault $f_k^{l_3}$; where $l_2 \geq l_3$.

The set of all components on which C_p^l is dependent is denoted as $DEP(C_p^l)$. Definitions 5.2.1 and 5.2.2 imply that we represent the dependencies among the different components within a particular level l at the next higher level $l + 1$. Note that a component C_p^l is dependent on itself; consequently, $C_p^l \in DEP(C_p^l)$. The following assumption regarding the component dependencies is now made explicit.

Assumption 5.2.1 (Component Dependency). Component dependencies are not considered for diagnosis at a component C_p^l with $pa(C_p^l) = \emptyset$.

Note that according to Definitions 5.2.1 and 5.2.2, dependencies of components and fault manifestations are directly related to each other. Furthermore, within an independent component C_p^l , it is useful to distinguish faults that are originated at C_p^l and those that are originated at some lower level but manifested at C_p^l . We decompose an independent component C_p^l into two virtual subcomponents, namely (1) *independent subcomponent of C_p^l* which is denoted by $D(C_p^l)$, and (2) *dependent subcomponent of C_p^l* which is denoted by $U(C_p^l)$ as shown in Figure 5.2. The faults that are originated at C_p^l correspond to $D(C_p^l)$ and those that are originated at lower level(s) but manifested at C_p^l correspond to $U(C_p^l)$. Once a component C_p^l is decomposed into the subcomponents $D(C_p^l)$ and $U(C_p^l)$, the subcomponents are treated as *independent* and *dependent* components, respectively. The dependencies among components are represented by directed arcs as shown in Figures 5.1 and 5.2. To represent dependencies, where $C_p^{l_1}$ is dependent on $C_q^{l_2}$, we add arcs from $C_q^{l_2}$ to $C_p^{l_1}$ and represent the arcs with an $n_{K'} \times n_K$ link matrix $L_{q,p}^{l_2,l_1}$ where $n_{K'}$ and n_K are the number of manifestable faults in $C_q^{l_2}$ and $C_p^{l_1}$, respectively. Each element of

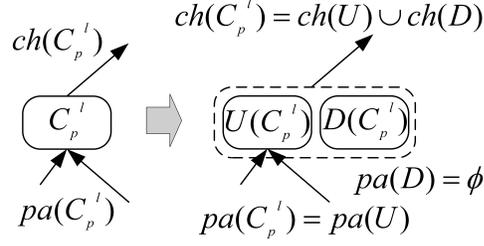


Figure 5.2: Decomposition of a component into “independent subcomponent” and “dependent subcomponent”.

the $L_{q,p}^{l_2,l_1}$ is denoted by $L_{q,p}^{l_2,l_1}(k', k)$, where $k' = 1, 2, \dots, K'$ and $k = 1, 2, \dots, K$. In this chapter, we assume that the dependencies are known with certainty. Consequently, given that a fault $f_{k'}^{l_2} \in C_q^{l_2}$ manifests in $C_p^{l_1}$ and identified as $f_k^{l_1} \in C_p^{l_1}$, then $L_{q,p}^{l_2,l_1}(k', k) = 1$. If two components are not dependent given the faults $f_{k'}^{l_2}$ and $f_k^{l_1}$, then $L_{q,p}^{l_2,l_1}(k', k) = 0$.

It follows from Definition 4.2.1 and the above discussion that the signature of an level l fault is not possible to be observed at lower levels, and the origin of an level l fault is in one of the “independent subcomponents” $D(C_p^l)$. It is important to note that in the graphical representation of Figure 5.2, $pa(U) \neq \emptyset$ and $pa(D) = \emptyset$, and it is possible that a component C_p^l where $l > 1$ does not have any “dependent subcomponent”. In practical sense this is possible due to lack/unavailability of an in-depth information about a subsystem or a component.

We propose to perform fault diagnosis at individual components in the hierarchical fault diagnosis model (HFDM) which are represented by nodes in Figures 5.1 and 5.2. We now formally define a fault diagnosis module (FDM) that corresponds to a node or component C_p^l as follows:

Definition 5.2.3 (FDM of a Component). A fault diagnosis module (FDM) corresponding to a component C_p^l is denoted by $FDM(C_p^l) = (S_p^l, F_{id,p}^l, R_{p,K}^l, \mathcal{O}_p^l, \mathcal{A}_p^l)$; where the diagnostic signals S_p^l are the inputs to the system, the identified faults $F_{id,p}^l$ are the outputs of the system, and the system is characterized by a set of

rules $R_{p,K}^l$ that describe the relations among the K faults and their corresponding symptoms, a set of operators \mathcal{O}_p^l that are utilized to compute the rule activation levels, and a set of assumptions \mathcal{A}_p^l that are made during the rule synthesis.

As described in Section 5.2.3, the rules $R_{p,K}^l$ are obtained from the corresponding fault signature model FSM_p^l .

5.2.2 Properties of the Proposed HFDM

In this section, the properties of the proposed hierarchical fault diagnosis model (HFDM) that is presented in Section 5.2.1 are emphasized. We state the properties of the model in terms of inputs, outputs and system properties of the FDMs (as defined in Section 5.2.1). The considered properties are as follows:

1. At level $l = 1$, between any two independent components C_p^1 and C_q^1 we have:
 - a. $S_p^1 \cap S_q^1 = \emptyset$
 - b. $F_p^1 \cap F_q^1 = \emptyset$
 - c. $R_{p,K}^1 \cap R_{q,K'}^1 = \emptyset$
2. At level l ($L > l > 1$), between any two components C_p^l and C_q^l we have:
 - a. $S_p^l \cap S_q^l = \emptyset$
 - b. $F_p^l \cap F_q^l = \emptyset$ if $C_p^l \in D(C_p^l)$ or $C_q^l \in D(C_q^l)$;
 $F_p^l \cap F_q^l \neq \emptyset$ if C_p^l and C_q^l are dependent, and $\exists f_k^{l-i} \in C_r^{l-i} \mid C_r^{l-i} \in \{DEP(C_p^l) \cap DEP(C_q^l)\}; l - i \geq 1$
 - c. $R_{p,K}^l \cap R_{q,K'}^l = \emptyset$
3. At the highest level $l = L$, only one component exist; i.e., C_p^L ; $p = P_1 = 1$.
4. At two different levels l_1 and l_2 , where $l_1 > l_2$, between any two components $C_p^{l_1}$ and $C_q^{l_2}$ the following relations hold:

- a. $S_p^{l_1} \cap S_q^{l_2} = \emptyset$
- b. $F_p^{l_1} \cap F_q^{l_2} = \emptyset$ if $C_q^{l_2} \notin DEP(C_p^{l_1})$;
 $F_p^{l_1} \cap F_q^{l_2} \neq \emptyset$ if $C_q^{l_2} \in DEP(C_p^{l_1})$
- c. $R_{p,K}^{l_1} \cap R_{q,K'}^{l_2} = \emptyset$

5. and finally we have $L_{q,p}^{l_2,l_1}(k',k) \in [0,1]$.

In the proposed HFDM, all the components C_p^l with $pa(C_p^l) = \emptyset$ are considered to be the “atomic” in the sense that identification of the location of faults beyond this level is not either deemed necessary or possible due to lack of the available information. Consequently, all the subsystem components, i.e., the sensors and the actuators are “atomic” components. Property-1 states that the diagnostic signals, manifestable faults, and the rules in two different atomic components are different. Note that the faults may be similar in two identical components (increase in friction in two different reaction wheels) but they are treated as different faults from fault localization perspective as their origins are different.

Property-2a states that the sets of diagnostic signals in two different components located at an intermediate level ($L > l > 1$) in the hierarchy are different (this is related to the fact that as mentioned above we represent the dependencies among different components within a particular level l at the next higher level $l + 1$). Consequently, the corresponding rule sets are also different (Property-2c). However, as Property-2b states, if both the components are dependent, sets of the manifestable faults in the two components may not be completely different if there exist a fault (originated at some lower level) that manifests in both the components.

Property-3 emphasizes that at the highest level, the entire system under consideration is represented by a single component. Property-4 states that between two different components located at two different levels, their properties are the same as that Property-1 of the components that are located at level 1 if the components

are not dependent on each other. Otherwise, there exist a fault (originated at the component located at the lower level or some other component(s) located at an even lower level) that manifests in both the components. Note that if $(l_1 - l_2) = 1$, i.e., in case of the components in two adjacent levels, it is possible— though not necessary— to have some diagnostic signals that are common to both $C_p^{l_1}$ and $C_q^{l_2}$. Finally, property-5 states that the inter-component fault dependencies are represented in the HFDM with absolute certainty while the uncertainties related to fault manifestations are taken into account in each FDM.

Note that in the hierarchical fault diagnosis approach that was presented in [19], the concept of “level l fault” was not considered in their formulation and the approach is too restrictive in the sense that it allowed only Property-1 to be true for any two given components in the hierarchy. Consequently, the overall applicability of that structure is very limited in the presence of components with higher degree of interactions.

5.2.3 Diagnosis of Faults in Independent Components at Level l

The fault diagnosis methodology described below is intended for a single component/subsystem C_p^l (the p -th component at level l) with relatively small or manageable number of diagnostic signals. Furthermore, the assumption of a single fault (no simultaneous faults) is made which is reasonable if the component/subsystem is monitored frequently. The problem of multiple faults will be addressed below in Section 5.2.4 where the single fault assumption is not realistic; for example, in the formation component at level L , faults may be present in more than one satellite at any given time.

First, consider the components that are located at the lowest level (level 1) in the hierarchy. The components C_p^1 s, at level 1, are independent according to

Proposition 5.2.1 below.

Proposition 5.2.1 (Independence of Level 1 Components). Each component C_p^1 located at level 1 is independent.

Proof. The proof directly follows from Definitions 5.2.1, 5.2.2, and Assumption 5.2.1 since in this case, $pa(C_p^1) = \emptyset, \forall p$. □

According to the properties that are stated in Section 5.2.2, the corresponding sets of diagnostic signals S_p^1 are different from each other and the faults in one component do not manifest in another component (this also implies that the components' health is monitored frequently enough and the FSMs are designed to identify faults that are of low severity). For example, a fault occurring at the Y-axis reaction wheel (subsystem component) in a 3-axes active attitude control subsystem would manifest within its own diagnostic signals before affecting the performance along the other two axes.

In the remaining part of this section, we identify the level with l instead of the fixed value 1 because the methodology, in general, is applicable to any component at a higher level as long as the component does not have any dependent subcomponents as described above. Note that in the absence of a dependent subcomponent, the properties of a component C_p^l becomes identical to that of an independent component that is located at level 1 (property 2.b in Section 5.2.2). Consider an independent component at level l . Let F_p^l be a finite set of K faults under consideration that is associated with a component C_p^l at level l : $F_p^l = \{f_k : k = 1, \dots, K\}$. Also let $S_p^l = \{S_{p,j}^l : j = 1, \dots, J\}$ be a finite collection of J sets of diagnostic signals. Each $S_{p,j}^l$ is obtained by extracting a feature from the available process states and/or variables (measured or calculated).

Next, we propose to perform fuzzy rule-based diagnosis [121] by utilizing the diagnostic signals defined above. In the general case, for a given fault f_k^l and N

diagnostic signals s_n^l , the objective is to synthesize fuzzy rule(s) in the following form:

$$\text{If } (s_1^l \in M_{1,k}^l) \text{ and } (s_2^l \in M_{2,k}^l) \dots \text{ and } (s_N^l \in M_{N,k}^l) \text{ then } f_k^l \quad (5.1)$$

where $M_{n,k}^l$ is a (set of) value(s) of the n -th diagnostic signal (characterized by the fuzzy membership function(s)) under the fault f_k .

Therefore, for fuzzy rule-based reasoning, we assign finite number of possible values to each of the above-mentioned diagnostic signal $s_{p,j}$ where each possible value is characterized by a fuzzy membership function (MF). Consequently, each diagnostic signal $s_{p,j}^l \in S_p^l$ can have a set of M possible values (M -valued fuzzy quantization of a feature) represented by the set $V_{s_{p,j}^l} = \{v_1, v_2, \dots, v_M\}$. Note that the number of elements in $V_{s_{p,j}^l}$ that is associated with each s_j^l need not necessarily be the same. Each possible value corresponds to a fuzzy set that is characterized by a membership function, namely $\mu_m(s_{p,j}^l = v_m) \in (0, 1)$.

Let $M_{p,j,k}^l$ denote the *fault manifestation* set (in terms of the diagnostic signal $s_{p,j}^l$) associated with the fault $f_k^l \in F_p^l$. Therefore, $M_{p,j,k}^l$ consists of the “values” in $V_{s_{p,j}^l}$ that indicate the presence of the fault f_k^l . Let M_p^l denote the collection of all possible fault manifestations; i.e., the values of all diagnostic signals under all the faults that are being considered.

Relations between faults and symptoms are expressed in the form of *if-then* rule sets $R_{p,K}^l$ within which the rule $r_{p,k}^l$ is represented as:

$$\begin{aligned} r_{p,k}^l \in R_{p,K}^l : \text{ If } (s_{p,1}^l \in M_{p,1,k}^l) \text{ and } (s_{p,2}^l \in M_{p,2,k}^l) \\ \dots \text{ and } (s_{p,J}^l \in M_{p,J,k}^l) \text{ then } (f_k^l) \end{aligned} \quad (5.2)$$

Premise fulfillment factor [84] is determined as follows:

$$\mu(s_{p,j}^l \in M_{p,j,k}^l) = \mu_1(s_{p,j}^l = v_1) \oplus \dots \oplus \mu_M(s_{p,j}^l = v_M) \quad | \quad v_m \in M_{p,j,k}^l \quad (5.3)$$

where the symbol \oplus represents the fuzzy sum operator, for example, s -norm operator such as MAX or drastic sum [121]. The activation level for the rule corresponding to the k -th fault is given by:

$$\mu(f_k^l) = \mu(s_{p,1}^l \in M_{p,1,k}^l) \otimes \dots \otimes \mu(s_{p,j}^l \in M_{p,j,k}^l) \otimes \dots \otimes \mu(s_{p,J}^l \in M_{p,J,k}^l) \quad (5.4)$$

where the symbol \otimes represents the fuzzy conjunction operator, for example, t -norm operator such as MIN or PROD [19, 121]. The use of a pre-defined rule activation threshold can be avoided by utilizing an “aggregation” operation to combine the results of all the rule activations in the FDM. For example, if the well-known “max” operator is used for aggregation, the fault with the maximum rule activation level can be considered as the identified fault (the output of C_p^l 's FDM as defined in Definition 5.2.3) in the component C_p^l as follows:

$$F_{id,p}^l = \{f_k^l : \mu(f_k^l) = \max [\mu(f_1^l), \dots, \mu(f_K^l)]\} \quad (5.5)$$

Note that in addition to the rules that are associated with different faults, one or more rules corresponding to the healthy conditions are possible to be included in the FDM. Finally, note that for two identical components C_p^l and C_q^l at the same level l , the sets of possible faults F_p^l and F_q^l , and the diagnostic signals $S_p^l \in C_p^l$ and $S_q^l \in C_q^l$ will be similar. Therefore, the FDMs of the two components can be constructed by following similar procedures which minimizes the design and development efforts, and allows re-use of software codes with minimal changes in the implementation stage.

Fault Identifiability: Note that two faults $f_k^l \in F_p^l$ and $f_{k'}^l \in F_p^l$ are always identifiable or distinguishable in a given FDM if $S_{p,j,k}^l \cap S_{p,j,k'}^l = \emptyset$; i.e., the faults are diagnosed based on disjunctive sets of diagnostic signals that are sensitive to specific faults.

However, when limited number of diagnostic signals are available from a component (due to the hierarchical decomposition), in the most difficult case where $S_{p,j,k}^l = S_{p,j,k'}^l$, the following condition is necessary for isolating or distinguishing two faults in a FDM:

$$\exists s_{p,j}^l \in (S_{p,j,k}^l \cap S_{p,j,k'}^l) : \max[\mu_m |_{v_m \in M_{p,j,k}} \cap \mu_{m'} |_{v_{m'} \in M_{p,j,k'}}] = \epsilon \quad (5.6)$$

where v_m and $v_{m'} \in V_{s_{p,j}^l}$ and “max” determines the maximum possible degree of membership of a diagnostic signal to the overlapping parts of μ_m and $\mu_{m'}$. Note that $\epsilon \in (0, 1)$ and as $\epsilon \rightarrow 0$, the degree of isolability becomes higher reaching the maximum level of isolability at $\epsilon \approx 0$. It should be noted here that if $s_{p,j}^l$ is associated with a complex premise (more than one value in $M_{p,j,k}$ and/or $M_{p,j,k'}$) in the signature of f_k^l and/or $f_{k'}^l$, the union of μ s is to be taken into consideration in (5.6) instead of μ_m and/or $\mu_{m'}$, and the intersection is to be computed on the union(s). Finally, for K faults in the FSM, each fault is distinguishable from all other faults if (5.6) holds for any given pair of faults $\langle f_k^l, f_{k'}^l \rangle \in F_p^l$.

5.2.4 Diagnosis of Faults in Dependent Components at Level

l

The fault diagnosis methodology and the conditions for fault isolability presented in Section 5.2.3 lead to simplicity in the fault isolation process. These are effective for

a specific component or subsystem with few faults and diagnostic signals. The proposed hierarchical framework allows us to utilize this methodology since we decompose the overall complex formation flying system into different components so that the problem of fault diagnosis in individual components becomes simpler. Furthermore, the assumption of single or non-simultaneous faults is reasonable especially at the lower levels in the hierarchy because it is very unlikely that a single component (such as an actuator) would develop two different faults at exactly the same time. When we take into consideration faults occurring at two different components (*multiple faults* within a subsystem or system or formation level), the effectiveness of the methodology in Section 5.2.3 becomes dependent on the extent of interactions between the two components as well as the fault severity which may result in manifestations (of a fault occurring at one component) in a different component.

Identical components C_p^l and C_q^l at the same level with higher degree of interactions require special attention. A particular case of one's interest will be the highest level L (the "formation" level) where the component consists of individual satellites within the leader-follower type satellite under consideration. It is important to note that one of the main objectives of the satellite formation flight is to maintain some pre-specified relative attitude/orientations of the satellites in space so that mission goals can be accomplished. When the interactions of the satellites are characterized by the well-known leader-follower (LF), or the master-slave control architecture (refer to Section 3.2.1 for a detailed description), the leader satellite is commanded by the ground station to maintain some specific attitude with respect to the Earth-fixed inertial frame, and the followers are commanded by the leader to maintain some specific attitude with respect to its body-fixed reference frame. Usually, there is no control feedback from the followers to the leader. Furthermore, the sensors that utilize advanced technologies such as optical metrology are capable of measuring relative attitude with high precision. Consequently, faults are expected

to have clearer manifestations in relative measurements. From the fault diagnosis perspective, when diagnostic signals correspond to the relative measurements, the above type of control architecture implies that a fault in a follower satellite would manifest in a set diagnostic signals that is related to the specific follower.

Based on the above discussion, in this thesis the diagnostic signals in dependent components are the features extracted from the relative state measurements. The faults that occur in spacecraft are mostly related to the subsystem components. In the subsequent discussion, we consider a general problem of fault diagnosis where the origins of faults f_k^l are at some low level l but have manifestations (denoted by $M_{j,k}^L$) at the highest level L . It should be clear that the primary fault diagnosis objective at level L is to identify the formation component(s) (individual satellites) that is/are faulty.

Let $C^L = \{C_p^L : p = 1, \dots, P\}$ denote a set of P components whose dependencies and interactions are characterized by the well-known leader-follower (LF), or the master-slave control architecture; where $p = 1$ corresponds to the single leader in the set. We assume that $P \geq 3$, where for $P = 3$ follower components can obtain relative state measurements with respect to each other. Furthermore, let $S_{pq}^L = \{S_{pq,j}^L : j = 1, \dots, J\}$ be a finite collection of J sets of diagnostic signals at level L where each $S_{pq,j}^L$ is obtained by extracting a useful feature from relative state measurements; i.e., $s_{pq,j}^L \in S_{pq}^L$ corresponds to the j -th diagnostic signal that is obtained from a relative measurement of C_p^L with respect to C_q^L . Furthermore, let the manifestation set of a fault f_k^l occurring at C_p^L in terms of $s_{pq,j}^L \in S_{pq}^L$ be denoted by $M_{pq,j,k}^L$. Manifestations corresponding to a healthy condition is represented by $M_{pq,j,0}^L$.

Assumption 5.2.2 (Uncertainty in the Diagnostic Signal Values).

Diagnostic signal values corresponding to the healthy and faulty relative state behavior are uncertain; i.e., adjacent fuzzy membership functions are overlapped.

Assumption 5.2.2 implies that we are interested in realistic systems in which uncertainty is dominant, and fault manifestations are not clear. Note that the assumption has been made explicit because it is not always the case that the adjacent fuzzy members are overlapped.

Proposition 5.2.2 (Non-unique Fault Signatures at Higher Levels).

With limited number of diagnostic signals at higher levels, multiple non-simultaneous faults originated at different lower level components may have the same manifestation(s) at some higher level component.

Proof. Let a set of lower level components in the proposed HFDM be denoted by $C_1^l, \dots, C_{P_l}^l$, where $l = 1, 2, \dots, l + i - 1$; and a higher level component be denoted by C_q^{l+i} . According to the proposed hierarchical structure of HFDM, if $\{C_1^l, \dots, C_p^l, \dots, C_{P_l}^l\} \in DEP(C_q^{l+i})$, there exist an (sequence of) arc(s) from each C_p^l to the component C_q^{l+i} where the arcs represent dependencies in observed fault signatures. Therefore, manifestations of faults originated at level l can be observed in C_q^{l+i} at level $l + i$. Now, if the number of diagnostic signals in C_q^{l+i} are fewer than the number of components and the associated faults at level l , construction of an FSM with rules that can uniquely identify each fault originated at level l will not be feasible. □

Proposition 5.2.3 (Faults in the Leader). If the diagnostic signals at level L correspond only to the relative state information, the faulty component C_1^L , where C_1^L is the leader component, cannot be identified at level L .

Proof. The proof is based on facts that are related to the structure of the proposed HFDM as well as that of the leader-follower control configuration where the leader acts as a “reference point”. In the proposed HFDM, interactions among the components are represented by a single node at level L . In the presence of an incorrect reference behavior, the followers simply follow the behavior and the relative states

are maintained. Consequently, the diagnostic signal values v_m remain healthy; i.e., $v_m \in M_{pq,j,0}^L, \forall p, q$. \square

It should be noted that although the faults that originate in the *leader component* are not identifiable at level L by utilizing only the relative state information, they can be identified either at lower levels FDMs (according to Definition 4.2.1), or by a human supervisor (can be considered as a supervisory diagnoser at level $L + 1$) at ground station by checking if the leader conforms to the pre-determined specifications.

We propose the following fuzzy inference rule for identifying the faulty *follower component* in the formation by utilizing diagnostic signals corresponding to the level L , namely

$$\begin{aligned} \text{If } (s_j^L \mid_{s_j^L \in S_{p1}^L} \in M_{p1,j,k}^L) \text{ and } (s_j^L \mid_{s_j^L \in S_{pp^*}^L} \in M_{pp^*,j,k}^L) \\ \text{and } (s_j^L \mid_{s_j^L \in S_{p^*1}^L} \in M_{p^*1,j,0}^L) \text{ then } \{f_k^l\} \end{aligned} \quad (5.7)$$

where $p \neq 1$ and p^* corresponds to a single follower component that is an active neighbor to C_p^L . By “active neighbor to C_p^L ” we imply a follower component with respect to which the state measurements of C_p^L are available. Note that the rule in (5.7) utilizes diagnostic signals that correspond to multiple relative state measurements, and helps restricting the undesired rule activations that would lead to persistent false and/or missed fault identification (refer to Assumption 5.2.2). Furthermore, the consequent part of the rule in equation (5.7) represents a set of faults (the output of C_p^L 's FDM as defined in Definition 5.2.3) rather than a single fault because at higher levels fault manifestations may be the same for a set of faults originated at some lower level (according to Proposition 5.2.2). The activation level of the rule in (5.7) is computed as that in (5.4).

The above methodology is applicable to any component whose subcomponents'

interactions are characterized within a leader-follower (LF), or the master-slave control architecture at a given level l . We propose to utilize the methodology that is presented in Section 5.2.3 along with the hierarchical fault diagnosis algorithm that is presented below for fault diagnosis in the dependent subcomponents that are not subjected to a master-slave type control configuration at a given level l .

Fault Identifiability: By fault identifiability or distinguishability at level L we refer to the conditions under which faults in multiple satellites can be identified. It is implicit in (5.7) that (a) the leader C_1^L is fault free, and (b) the follower $C_{p^*}^L$ is fault free. However, the assumption (a) can be relaxed for the rule in (5.7) if the following condition is satisfied in presence of non-simultaneous faults f_k^l in C_p^L and $f_{k'}^l$ in the leader. In other words, in the presence of a fault $f_{k'}^l$ in the leader,

$$s_j^L \mid_{s_j^L \in S_{p1}^L} \notin M_{p1,j,k}^L \quad \forall p, \quad p \neq 1 \quad (5.8)$$

The above condition ensures that leader's faults are not manifested sufficiently in the followers. Furthermore, assumption (b) above can be relaxed for the rule in (5.7) if the following conditions are satisfied in presence of simultaneous faults f_k^l in C_p^L and $f_{k'}^l$ in C_q^L (another follower), in other words,

$$C_p^L \notin q^*, \quad C_q^L \notin p^* \quad \text{and} \quad \{C_p^L, C_q^L\} \notin n^* \quad (5.9)$$

where p^* , q^* and n^* represent the active neighbors of C_p^L , C_q^L , and a given healthy satellite, respectively.

5.2.5 Rule-Based Hierarchical Fault Diagnosis

In general, for all the components (both the dependent and the independent sub-components) in the hierarchy, we propose to execute the following algorithm that

is designated as the **HierarchicalFD** in the FDM (per the Definition 5.2.3). Note that in the algorithm input, HFDM consists of information about the fault signature models as well as the dependency information of all the components.

Algorithm: HierarchicalFD($HFDM, \text{Detection alarm at } C_p^l$)

Initialization: $F_{id,p}^l(C_p^l) = \emptyset$ for all p and l

ComponentFD($HFDM, p, l$)

{

1. Identify the fault f_k^l by following the procedure in Section 5.2.3 or Section 5.2.4 (if C_p^l is a follower component).

2. **If** $f_k^l \in D(C_p^l)$, add f_k^l to $F_{id,p}^l(C_p^l)$ and STOP.

Else ($f_k^l \in U(C_p^l)$)

a. Add f_k^l to $F_{id,p}^l(C_p^l)$

b. For all $L_{q,p}^{l-1,l}(k', k) = 1$ and $L_{p,q}^{l,l+1}(k, k') = 1$,

execute **ComponentFD**($HFDM, q, l - 1$) and

ComponentFD($HFDM, q, l + 1$) in order to identify faults $f_{k'}^{l-1}$ and

$f_{k'}^{l+1}$, respectively.

End

}

Output: (1) Updated $F_{id,p}^l(C_p^l)$ s of the FDMs that execute the algorithm, and (2) Fault propagation path(s) $C_p^{l-i} \rightarrow C_p^l \rightarrow C_p^{l+1}$ (refer to Section 4.4) that is/are constructed by taking into account all the components with $F_{id,p}^l(C_p^l) \neq \emptyset$.

Note that the algorithm finds the origin of a fault by observing the fault signatures in the top-down direction when it executes **ComponentFD** ($HFDM, q, l - 1$)

and stops when it observes a fault signature in an independent sub-component. On the other hand, when it executes **ComponentFD** ($HFDM, q, l + 1$) in the bottom-up direction, it finds the manifestation of the fault in higher levels in order to determine the impact of the fault at higher levels.

Lemma 5.2.1 (Hierarchical Diagnosis).

When the proposed HFDM is known, the *HierarchicalFD* algorithm identifies the origin of the non-simultaneous faults whose signature models are available.

Proof. Let C_p^l be a component at level l ; where $L > l > 1$, in which a fault detection alarm is observed. According to the proposed HFDM, the origin of fault (f_k) is at level l_o ; where $l \geq l_o$ (by Definition 4.2.1). Now, if the origin of the fault is at level l , then $f_k^l \in D(C_p^l)$ (originated at an independent subcomponent) and the algorithm stops after identifying $f_k^l \in F_{id,p}^l(C_p^l)$. Otherwise, **ComponentFD**($HFDM, q, l - 1$) executes based on the fault signatures that are observed at C_p^l and the dependency information $L_{q,p}^{l-1,l}$. The process continues until a fault signature is observed at level l_o in an independent subcomponent. □

It is important to note that an exceptional scenario is possible where a fault is observed at higher level(s) but not observed at lower level(s) if the FDMs of the lower level(s) components are not “complete” in terms of observable faults (assuming dependency information is correct), which is contradictory to the basic definitions and assumptions (refer to Definition 5.2.2, and the discussion on HFDM in Sections 5.2.1 and 5.2.2) of the proposed HFDM.

5.2.6 Specification of the Fuzzy Membership Functions

The fault diagnosis methodology presented in Sections 5.2.3 and 5.2.4 can be extended for faults with a range of severity if it is possible to construct manifestation sets ($M_{p,j,k}^l$ s or $M_{pq,j,k}^l$ s) that correspond to a range of severity of fault f_k^l as opposed

to a specific severity. This “target severity range” is decided based on a worst-case analysis as well as by determining a minimum fault severity that is desired to be isolated and/or have impact on the system performance.

We propose to perform fault diagnosis over some qualitative time-window; for example by utilizing 1 orbit data and by invoking the proposed rule-based diagnosis multiple times within this interval. The fault diagnosis methodology presented in Sections 5.2.3 and 5.2.4 requires that each diagnostic signal ($s_{p,j}^l$ or $s_{pq,j}^l$) be represented by an M -valued quantization using the fuzzy sets where each value v_m (as discussed in Section 5.2.3) is characterized by a membership function (MF) denoted by μ_m . To avoid complete dependency on a human expert’s subjective judgement, for each diagnostic signal we propose to generate a set of M Gaussian membership functions whose total number M and the parameters (mean and standard deviations of each MF) are specified as follows:

1. Decide the “universe of disclosure” over which μ_m s are to be specified: the target severity range (as discussed above) is determined for all the faults under consideration and the range of $s_{p,j}^l$ (or $s_{pq,j}^l$) is identified.
2. Specify μ_m , where $m = 1 + ((M - 1)/2)$ is specified by obtaining its mean ($mean_{nom}$) and standard deviations (σ_{nom}) by utilizing healthy data. Select M to be a sufficiently large odd number so that the MFs (determined in Step-3) are spanned over the entire universe of disclosure (as determined in Step-1) equally toward both increasing and decreasing directions from $mean_{nom}$.
3. Construct μ_m s for $m = 1, 2, \dots, M$ ($m \neq 1 + ((M - 1)/2)$) by specifying $(M - 1)/2$ Gaussian membership functions that are spanned over the universe of disclosure (identified in Step-1) toward the increasing direction from $mean_{nom}$ that are $\delta_{mean} = \alpha\sigma_{nom}$ apart; where α is a design parameter and $\sigma_m = \sigma_{nom}$. For $m = 1$ and $m = M$, $\mu_m(x) = 1$ for $x \leq mean_1$ and $x \geq mean_M$,

respectively. Specify the remaining $(M - 1)/2$ Gaussian membership functions toward the decreasing direction from $mean_{nom}$.

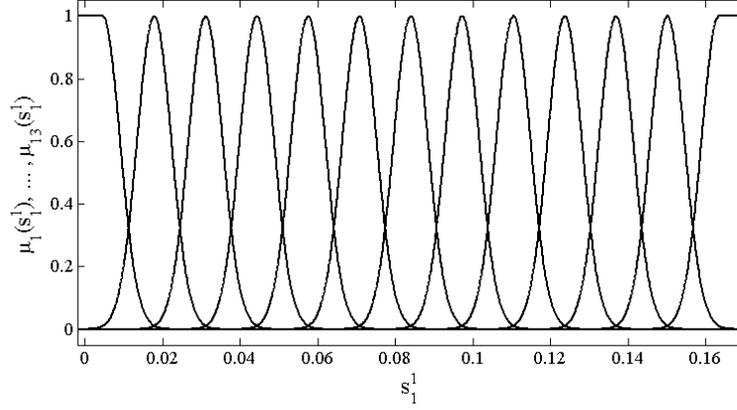


Figure 5.3: A set of Gaussian membership functions representing 13-valued quantization of the diagnostic signal s_1^1 (“mean of motor current”).

Figure 5.3 shows a set of fuzzy membership functions corresponding to the diagnostic signal “mean of motor current”, denoted by s_1^1 , with $M = 13$, $mean_{nom} = 0.0840$, $\sigma_{nom} = 0.0044$ and $\delta_{mean} = 0.0132$ ($\alpha = 3$).

5.3 Demonstration of the Proposed Approach and Fault Diagnosis Results

A 4-level hierarchical decomposition of the leader-follower formation flight of 5 satellites, as described in Chapter 3, results in the HFDM that is shown in Figure 5.4 where “Sat-1” ... “Sat-5” represent the five satellites in the formation, and “RW-X”, “RW-Y”, and “RW-Z” represent the reaction wheels (RW) in the X , Y , and Z directions, respectively. At level 1 (identified as the “subsystem component level”), each of the 15 RWs is denoted by C_p^1 ; where $p = 1, \dots, 15$. At level 2 (identified as the “subsystem level”), each of the 5 attitude control subsystems (ACS) node is denoted by C_p^2 ; where $p = 1, 3, 5, 7, 9$. Furthermore, each of the 5 electrical power

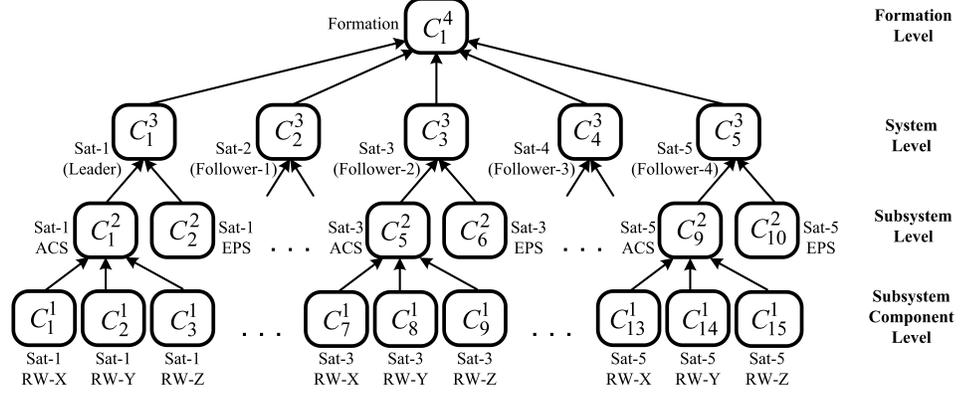


Figure 5.4: The HFDM that resulted from a 4-level hierarchical decomposition of the formation flight of satellites as described in Chapter 3 (shown in Figure 3.1).

subsystem (EPS) node is denoted by C_p^2 ; where $p = 2, 4, 6, 8, 10$ at level 2. At level 3 (identified as the “system level”), each of the 5 satellites is denoted by C_p^3 ; where $p = 1, 2, \dots, 5$, and at level 4, the entire formation flying system is represented with a single node C_1^4 .

In the subsequent paragraphs, we demonstrate the proposed fuzzy rule-based fault diagnosis (refer to Sections 5.2.3 and 5.2.4) for the following components of Figure 5.4, namely the 15 RWs (C_1^1, \dots, C_{15}^1) at level 1, the five EPSs ($C_2^2, C_4^2, C_6^2, C_8^2, C_{10}^2$) at level 2, and the formation component (C_1^4) at level 4. Note that the RWs and EPSs are assumed to be the independent components since $pa(C_p^1) = \emptyset, \forall p$ and $pa(C_p^2) = \emptyset$, for $p = 2, 4, 6, 8, 10$. On the other hand, the formation component C_1^4 is a dependent component. First, we discuss the level 1 faults and the level 2 faults that are injected in the independent components — the RWs and the EPSs — located at level 1 and level 2, respectively

Faults corresponding to each RW are denoted by $F_p^1 = f_{k,p}^1$; where $p = 1, \dots, 15$ and $k = 1, 2$. For $k = 1$, $f_{1,p}^1$ represents a *friction fault* in the p -th RW, and for $k = 2$, $f_{2,p}^1$ represents a *motor current fault* in the p -th RW (fault modes are described in Section 3.5). Faults corresponding to each EPS are denoted by $F_p^2 = f_{k,p}^2$; where $p = 2, 4, 6, 8, 10$; $k = 1, 2$. For $k = 1$, $f_{1,p}^2$ represents a *voltage regulation fault* in the

p -th EPS, and for $k = 2$, $f_{2,p}^2$ represents a *battery fault* in the p -th EPS (fault modes are described in Section 3.5). Note that the two EPS faults are level 2 faults.

Note that we have not considered any level 2 fault in the ACS. Consequently, the faults corresponding to the five ACSs (C_p^2 , where $p = 1, 3, 5, 7, 9$) are as follows: $F_p^2 = \bigcup_q F_q^1$ with $p = 1, 3, 5, 7, 9$ and q identifying a RW within a particular ACS. As an example, according to the HFDM schematic in Figure 5.4, for $p = 1$, the corresponding qs are $\{1, 2, 3\}$; for $p = 5$, the corresponding qs are $\{7, 8, 9\}$, and so on. Alternatively, the 6 faults (friction and motor current faults in 3 RWs) of level 1 can be identified as “RW-X fault”, “RW-Y fault” and “RW-Z fault” in the ACS at level 2, if necessary. Furthermore, at this stage, we have not considered any level l ($l \geq 3$) fault. Consequently, the fault sets corresponding to the higher level ($l \geq 3$) components do not consist of any new fault.

Diagnosis of Faults in Independent Components at Level 1: For subsystem component level fault diagnosis in each of the 15 RWs, diagnostic signals are obtained by extracting features from the following RW measurements: (a) motor current, (b) torque command voltage, and (c) wheel speed. Based on the earlier experience with an actual attitude control subsystem telemetry data [43], we have extracted ten features that include (over an invocation window of 512 seconds; approximately 11 invokes per orbit) *mean, standard deviation, minimum value, peak value, energy*, and the first 5 *components of the Fast Fourier Transform (FFT) energy spectrum*. Out of all the features it is found that it is possible to obtain manifestations of the current fault as well as the friction fault within the target severity range (as indicated in Section 5.2.6) with the following three diagnostic signals: (1) $s_{p,1}^1$: *mean* of motor current, (2) $s_{p,2}^1$: *mean* of torque command voltage, and (3) $s_{p,3}^1$: the *first component of the FFT* of the wheel speed. The set of diagnostic signals that are selected for rule-based reasoning is $S_p^1 = \{s_{p,1}^1, s_{p,2}^1, s_{p,3}^1\}$; where p identifies a specific

RW.

By following the procedure that is described in Section 5.2.3, we have assigned a finite number of possible values to each diagnostic signal in S_p^1 by performing an M -valued fuzzy quantization where $M = 13$ for $s_{p,1}^1$ and $s_{p,2}^1$, and $M = 11$ for $s_{p,3}^1$. Therefore, the set of possible values of $s_{p,1}^1$, $s_{p,2}^1$, and $s_{p,3}^1$ are: $V_{s_{p,1}^1} = \{v_1, \dots, v_{13}\}$, $V_{s_{p,2}^1} = \{v_1, \dots, v_{13}\}$, and $V_{s_{p,3}^1} = \{v_1, \dots, v_{11}\}$, respectively. Note that these possible values, as well as the value of M for each $s_{p,j}^1$, are characterized by Gaussian membership functions which are specified by following the procedure outlined in Section 5.2.6. For the possible values μ_s of the three diagnostic signals we have selected $\sigma_m = 0044, 0.0232, 23.75$, respectively; and $\delta_{mean} = 0.0132, 0.0696, 71.26$, respectively (with $\alpha = 3$ chosen for all the three signals).

Finally, the fuzzy rules $r_{p,k}^1$ (as in equation (5.2)) for the RWs corresponding to the healthy RW condition as well as to the two faults under consideration are determined. Note that in $r_{p,k}^1$, $p = 1, \dots, 15$ and $k = 0, 1, 2$ where p identifies a specific RW, and $k = 0, 1$ and 2 represent the “healthy condition”, the *friction fault*, and the *motor current fault*, respectively. Fault manifestation sets $M_{p,j,k}^1$ (with $j = 1, 2, 3$ representing the diagnostic signals $s_{p,j}^1$) corresponding to the healthy as well as under the two faults are determined as follows:

$$\begin{aligned}
M_{p,1,0}^1 &= \{v_6, v_7, v_8\}, v_m \in V_{s_{p,1}^1} \\
M_{p,1,1}^1 &= \{v_8, v_9, v_{10}\}, v_m \in V_{s_{p,1}^1} \\
M_{p,1,2}^1 &= \{v_{11}, v_{12}, v_{13}\}, v_m \in V_{s_{p,1}^1} \\
M_{p,2,0}^1 &= \{v_6, v_7, v_8\}, v_m \in V_{s_{p,2}^1} \\
M_{p,2,1}^1 &= \{v_8, v_9, v_{10}\}, v_m \in V_{s_{p,2}^1} \\
M_{p,2,2}^1 &= \{v_{11}, v_{12}, v_{13}\}, v_m \in V_{s_{p,2}^1} \\
M_{p,3,0}^1 &= \{v_4, v_5, v_6\}, v_m \in V_{s_{p,3}^1} \\
M_{p,3,1}^1 &= \{v_7, v_8, v_9\}, v_m \in V_{s_{p,3}^1} \\
M_{p,3,2}^1 &= \{v_{10}, v_{11}\}, v_m \in V_{s_{p,3}^1}
\end{aligned}$$

The rule activations in each invoke are computed by using equation (5.4) and the well-known *max* operator is used to “aggregate” the rule activation results in order to generate a final diagnostic decision. Some sample rule activation results are provided at the end of this section.

Diagnosis of Faults in Independent Components at Level 2: The demonstration is similar to that of the RWs developed above expect for the diagnostic signals and the faults under consideration. Consequently, we briefly describe the procedure for the 5 EPSs at level 2. We have obtained the diagnostic signals by extracting features from the following EPS measurements, namely (a) the bus voltage, and (b) the regulator output current. We have extracted four features that include (over the above-mentioned invocation window of 512 seconds) *mean*, *standard deviation*, *minimum value*, and one selected *component of the Fast Fourier Transform (FFT) energy spectrum*. The set of diagnostic signals that was selected for the rule-based reasoning in EPSs is $S_p^2 = \{s_{p,1}^2, s_{p,2}^2, s_{p,3}^2, s_{p,4}^2, s_{p,5}^2, s_{p,6}^2\}$; where $s_{p,1}^2$, $s_{p,2}^2$, and $s_{p,3}^2$ are the *mean*, *standard deviation*, and the selected *component of FFT* of the bus voltage, respectively. Similarly, $s_{p,4}^2$, $s_{p,5}^2$, and $s_{p,6}^2$ are the corresponding features of the regulator output current.

By following the procedure that is described in Section 5.2.3, we performed an M -valued fuzzy quantization of the diagnostic signals in S_p^2 ($p = 2, 4, 6, 8, 10$). As in the RWs case, the procedure that is outlined in Section 5.2.6 was followed to determine M and the possible values of each $s_{p,j}^2$; i.e., $V_{s_{p,j}^2} = \{v_1, \dots, v_M\}$ with $j = 1, 2, \dots, 6$. The values of M are determined as follows: $M = 17$ for $\{s_{p,1}^2, s_{p,2}^2, s_{p,4}^2, s_{p,5}^2\}$ and $M = 19$ for $\{s_{p,3}^2, s_{p,6}^2\}$. Fault manifestation sets $M_{p,j,k}^2$ are identified (not shown here) and the fuzzy rules $r_{p,k}^2$ (as in equation (5.2)) for the EPSs corresponding to the healthy EPS condition as well as to the two faults under consideration are determined. We have, $p = 2, 4, 6, 8, 10$ and $k = 0, 1, 2$ where p identifies a specific EPS,

and $k = 0, 1$ and 2 represent the “healthy condition”, the *voltage regulation fault* and the *battery fault*, respectively. As in the case of the RWs, the rule activations in each invoke are computed for EPSs by using equation (5.4) and the well-known *max* operator is used to “aggregate” the rule activations results in order to generate a final diagnostic decision. Some sample rule activation results are provided at the end of this section.

Diagnosis of Faults in the Dependent Component at Level 4: For component fault diagnosis of the formation (C_1^4) , *mean of the relative attitude measurements* over an invocation window is utilized as the diagnostic signal and the rule in equation (5.7) is implemented for each follower satellite based on the formation configuration that is shown in Figure 3.1. Since the main objective of the formation level diagnosis is to identify the satellite(s) that is/are faulty, and since we have not considered any level 4 fault (as indicated above), we represent all the faults that are originated at lower levels with the finite set $F_1^4 = \{f_2, \dots, f_5\}$, where f_2, \dots, f_5 stand for “satellite-2 fault”, ..., “satellite-5 fault”, respectively (as explained in Section 5.2.4, the leader satellite is assumed to be fault free). The diagnostic signals are the relative attitude measurements. For example, the diagnostic signals $s_{pq,j}^4$ that are used in the rule for “satellite-2 fault” are:

1. $s_{21,1}^4$: *mean of the relative roll angle* of Sat-2 with respect to Sat-1 (leader)
2. $s_{21,2}^4$: *mean of the relative pitch angle* of Sat-2 with respect to Sat-1
3. $s_{21,3}^4$: *mean of the relative yaw angle* of Sat-2 with respect to Sat-1
4. $s_{23,4}^4$: *mean of the relative roll angle* of Sat-2 with respect to Sat-3 (active neighbor)
5. $s_{23,5}^4$: *mean of the relative pitch angle* of Sat-2 with respect to Sat-3

6. $s_{23,6}^4$: mean of the relative yaw angle of Sat-2 with respect to Sat-3
7. $s_{31,7}^4$: mean of the relative roll angle of Sat-3 with respect to Sat-1
8. $s_{31,8}^4$: mean of the relative pitch angle of Sat-3 with respect to Sat-1
9. $s_{31,9}^4$: mean of the relative yaw angle of Sat-3 with respect to Sat-1

For each diagnostic signal, an $M = 13$ -valued fuzzy quantization is performed and the fault manifestation sets $M_{p1,j,k}^4$, $M_{pp^*,j,k}^4$, and $M_{p^*1,j,0}^4$ of the rules in equation (5.7) are determined. As an example, for “satellite-2 fault”, the fault manifestation sets $M_{21,k}^4$, $M_{23,j,k}^4$, and $M_{31,j,0}^4$ correspond to the sets of diagnostic signals $\{s_{21,1}^4, s_{21,2}^4, s_{21,3}^4\}$, $\{s_{23,4}^4, s_{23,5}^4, s_{23,6}^4\}$, and $\{s_{31,7}^4, s_{31,8}^4, s_{31,9}^4\}$, respectively. Again, for simplicity, fuzzy MIN and MAX [121] operators are used as t -norm operator (\otimes) and s -norm operator (\oplus), respectively.

Sample Rule Activation Results: To demonstrate the proposed approach, we present below a case where we have injected the two faults in the subsystem component level simultaneously between $t = 7500$ s and $t = 9810$ s, namely (1) *friction fault* in the Z-axis reaction wheel of Sat-3, and (2) *motor current fault* in the Z-axis reaction wheel of Sat-5; within their “target severity range”. Note that although the faults are simultaneous, they are injected at two different satellites. Therefore, this case is consistent with the assumption of a single fault in subsystem components that was made in Section 5.2.3.

First, we present some sample rule activation results of level 1 components. Figure 5.5 shows the rule activations corresponding to the Sat-3 Z-axis reaction wheel under friction fault (injected between $t = 7500$ s and $t = 9810$ s) where $\mu(f_1^1)$ and $\mu(f_2^1)$ represent rule activation levels for the *friction fault* (f_1^1) and the *motor current fault* (f_2^1), respectively, and $\mu(H)$ represents the rule activation corresponding to the healthy RW condition. It is important to note that, as indicated above,

we extract features from data and perform fault diagnosis by using 512-second non-overlapping time window (approximately 11 invocations per orbit). Consequently, the width of each bar-graph in Figure 5.5 is 512 seconds. Similar rule activations

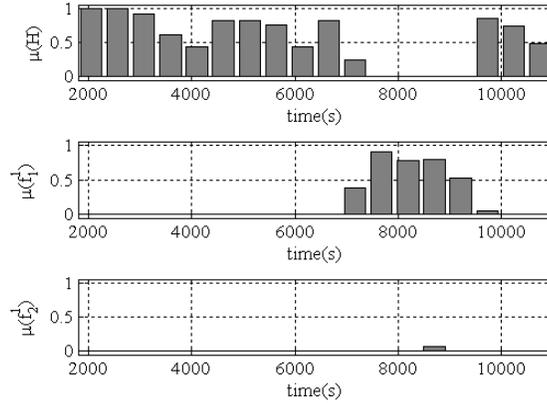


Figure 5.5: Rule activations in the Z-axis RW of Sat-3 under friction fault (the width of each bar-graph is 512 seconds).

are observed for the simultaneously injected *motor current fault* (injected between $t = 7500$ s and $t = 9810$ s) in the Sat-5 Z-axis reaction wheel as shown in Figure 5.6 with misidentification of faults (the friction fault is misidentified as the current fault) during the fault transients (the overall performance of fault diagnosis is quantified in the “performance evaluation” subsection provided in the subsequent discussions below). The rules associated with the remaining 13 reaction wheels did not (with a few exceptions which are discussed under “performance evaluation” in the subsequent discussion) fire to sufficient degrees that would lead to a “faulty” status after the “aggregation” (used for determining which rule has the maximum activation) of the rule firing results.

Next, we present some sample formation level rule activation results; i.e., rule activations at a dependent component. Figures 5.7 and 5.8 show the formation level rule activations under the above-mentioned simultaneous faults (injected at the subsystem component level) in Sat-3 and Sat-5 where $\mu(F)$ and $\mu(H)$ represent the

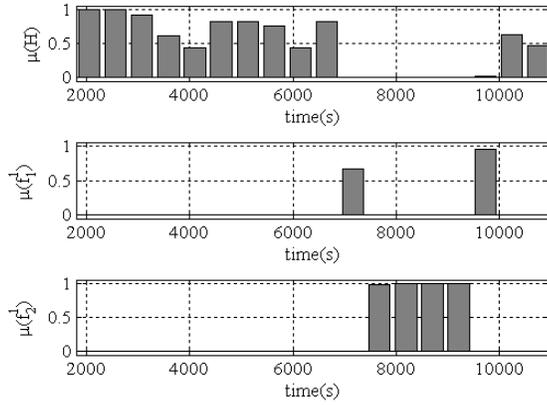


Figure 5.6: Rule activations in the Z-axis RW of Sat-5 under motor current fault (the width of each bar-graph is 512 seconds).

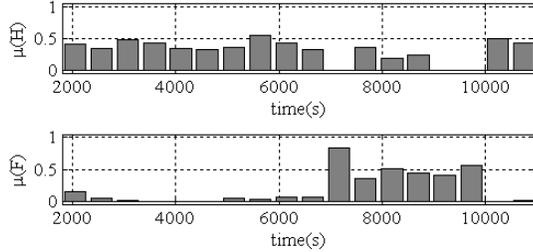


Figure 5.7: Rule activations that identify a “Sat-3 fault” (the width of each bar-graph is 512 seconds).

rule activations corresponding to a faulty and a healthy condition for a given satellite (formation component). The rule activations in Figures 5.7 and 5.8 demonstrate high level manifestations of low level faults and emphasize the usefulness of the “level l fault” concept.

Finally, we present some sample rule activation results for the independent components at level 2. Figure 5.9 shows the rule activations corresponding to the Sat-5 EPS under the battery fault (injected between $t = 6500$ s and $t = 6860$ s) where $\mu(f_1^2)$ and $\mu(f_2^2)$ represent the rule activation levels for the voltage regulator fault (f_1^2) and the battery fault (f_2^2), respectively, and $\mu(H)$ represents the rule activation corresponding to a healthy EPS condition.

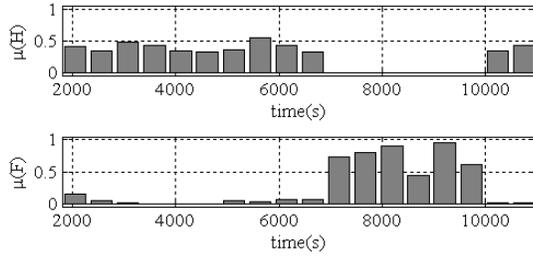


Figure 5.8: Rule activations that identify a “Sat-5 fault” (the width of each bar-graph is 512 seconds).

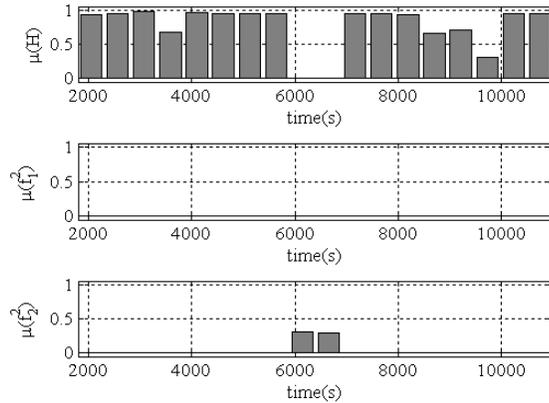


Figure 5.9: Rule activations in the EPS of Sat-5 under battery fault.

5.4 Performance Evaluation

In this section we evaluate the performance of the proposed fault diagnosis scheme by utilizing confusion matrices. The terms “confusion matrix” and “detection matrix”/“decision matrix” are sometimes used interchangeably in the literature. In this thesis we distinguish between the two matrices. As defined in [56] and [57], a detection matrix is square matrix of dimension 2 that is related to binary decision making or fault detection. Such matrices directly show the “false positives” (false alarms), “false negatives” (missed detection), etc. On the other hand a confusion matrix is a typically square matrix of dimension n that is utilized to evaluate fault identification or classification, where n is the number of health states. The healthy or “no-fault” cases can also be included in the confusion matrix. In the subsequent

Table 5.1: Confusion Matrix for the Subsystem Component Level

Identified → Actual ↓	Healthy	Friction Fault	Current Fault	Ambiguity
Healthy	169	3	0	0
Friction Fault	11	29	0	0
Current Fault	2	13	25	0

paragraphs we have added another extra column with the confusion matrices to accommodate ambiguous cases. For comparing two fault identification algorithms on a given data set, “kappa coefficients” [56,57] are computed from confusion matrices which is a measure of an algorithm’s ability to correctly classify a fault and takes into account the expected number of correct classifications occurring by chance. In this thesis our focus is on fault diagnosis or identification, and we are not going to compare the performances of two different algorithms on a given data set. Consequently, in this section we use overall accuracy [144] that is computed from a confusion matrix as a measure of performance.

It is important to note that in the subsequent paragraphs we construct 2×2 dimensional “one-versus-all” decision matrices in order to compute overall accuracy in fault identification. However, it should be clear that the information that these “one-versus-all” decision matrices provide are very different from what is available from a typical detection matrix or decision matrix that are used to evaluate fault detection performance. This is because the decision matrices that we construct in this thesis are “one-versus-all” as opposed to “healthy-versus-faulty”.

To quantify the performance of the proposed scheme confusion matrices are constructed corresponding to the rule activation results in the highest (formation level) and the lowest (subsystem component level) with unseen data. The data also included some cases where the fault severities were lower than the “target severity range” (as specified in Section 5.2.6).

Tables 5.1, 5.2 and 5.3 represent the confusion matrices corresponding to the

Table 5.2: Confusion Matrix for the Subsystem Level

Identified → Actual ↓	Healthy	Regulator Fault	Battery Fault	Ambiguity
Healthy	224	0	0	0
Regulator Fault	0	32	0	0
Battery Fault	0	0	24	0

Table 5.3: Confusion Matrix for the Formation (Followers) Level

Identified → Actual ↓	Sat-2 Fault	Sat-3 Fault	Sat-4 Fault	Sat-5 Fault	Healthy	Ambiguity
Sat-2 Fault	11	0	0	0	0	1
Sat-3 Fault	0	39	0	0	11	3
Sat-4 Fault	0	0	11	0	0	1
Sat-5 Fault	0	0	0	17	0	1
Healthy	0	2	0	2	281	0

subsystem component, subsystem, and the formation levels, respectively where the numbers correspond to the “number of invocation” over the above-mentioned 512 seconds time window. An “ambiguity” corresponds to a situation where two different rules (one corresponding to a healthy status and the other corresponding to a faulty status) have equal activation levels. In the subsystem component level, aggregated rule firing results are utilized to construct Table 5.1. In the formation level, the aggregation is performed within the individual satellite’s rule firing results. Table 5.4 shows the accuracy of the proposed scheme in the three levels under consideration. The accuracies have been computed by following the procedure that is available in [144]; i.e. first by decomposing the confusion matrices in Tables 5.1, 5.2, and 5.3

Table 5.4: Overall Fault Identification Accuracy

Formation Level	98.31%
Subsystem Level (Electrical Power Subsystem (EPS))	100%
Subsystem Component Level (Reaction Wheels (RW))	92.33%

into n numbers ($n = 3$ for Tables 5.1 and 5.2, and $n = 5$ for Table 5.3) of “one-versus-all” decision matrices and then summing the matrices to obtain a confusion matrix that represents the overall classification accuracy which is described next.

Let \mathbf{C}_{con} denote an $(N + 1) \times (N + 1)$ confusion matrix that is associated with $N + 1$ health states (the healthy state and the N number of faulty states) of a component at level l in which the actual and the identified health states are along the rows and the columns, respectively. To compute the accuracy in identifying the n -th state, a 2×2 dimensional “one-versus-all” decision matrix \mathbf{C}_n is constructed as follows. Let $c_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_{con} , and $c'_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_n . The elements of the \mathbf{C}_n matrix are computed from $c'_{2,2} = c_{n,n}$, $c'_{2,1} = (\sum_{k=1}^N c_{n,k}) - c_{n,n}$, $c'_{1,2} = (\sum_{k=1}^N c_{k,n}) - c_{n,n}$, and $c'_{1,1} = (sum(\mathbf{C}_{con}) - c'_{2,2} - c'_{2,1} - c'_{1,1})$. The accuracy of identifying the n -th state at level l is now defined as $a_n = trace(\mathbf{C}_n) / sum(\mathbf{C}_n)$. On the other hand, the overall accuracy is computed as follows. First the sum of the n number of “one-versus-all” decision matrices is computed as $\mathbf{C}_{ov} = \sum_{i=1}^n \mathbf{C}_n$. Then the overall fault identification accuracy at level l is defined as $a_{ov} = trace(\mathbf{C}_{ov}) / sum(\mathbf{C}_{ov})$.

It is observed in Tables 5.2 and 5.4 that fault identification accuracy at level 2 is 100% which may appear to be unrealistic. This high accuracy is due to the fact that the controller or simplified power distribution and control unit (PDCU) of the EPS is found to be very sensitive to the faults that are considered in this thesis. Consequently, fault manifestations were much clearer as compared to those in the subsystem component level or the formation level.

Comparing the formation level and the subsystem component level, the fault identification accuracy in the formation level is found to be higher (98.31%) than that of the subsystem component level (92.33%). The reason behind the higher fault identification accuracy in the formation level is that in cases of low severity faults, the formation level diagnosis is found to perform better than that of the subsystem

component level. This is due to the fact that faults are found to have clearer manifestations in relative measurements (as mentioned in Section 5.2.4) that are used to generate diagnostic signals in the formation level. For example, Figure 5.10 shows the rule activations in the Z-axis RW of Sat-3 under low severity (outside the target severity range as specified in Section 5.2.6) motor current fault that is injected between $t = 5800$ s and $t = 8110$ s. It is observed that the rules corresponding to both the friction fault and the motor current fault are activated in the subsystem component level. Therefore, the exact source of the fault cannot be identified. To investigate if these are false alarms, one can refer to Figure 5.11 which shows the formation level rule activations in the Sat-3 during the above-mentioned low severity motor current fault in the Z-axis RW of Sat-3. The rule activation is consistent and clear which confirms the presence of a fault in Sat-3 even though the source of the fault is not identified in the subsystem component level.

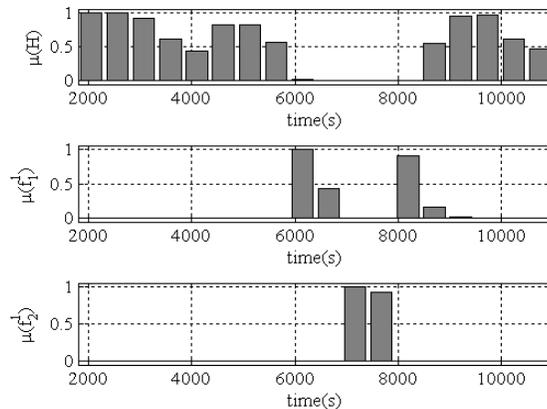


Figure 5.10: Rule activations in the Z-axis RW of Sat-3 under low severity motor current fault (the width of each bar-graph is 512 seconds).

Note that around $t = 6050$ s, the healthy rule activation $\mu(H)$ in Figure 5.11 is much lower than the “Sat-3 fault” rule activation $\mu(F)$.

Since the formation level diagnosis provides clearer identification of faults, it can certainly be utilized as a supervisory diagnosis system for the formation

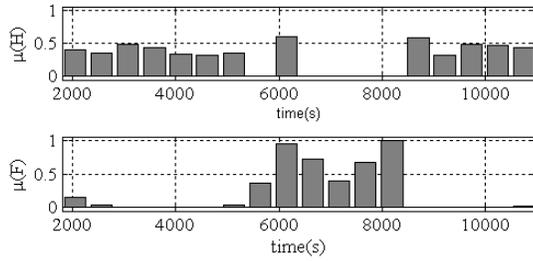


Figure 5.11: Formation level rule activations in the Sat-3 under low severity motor current fault injected at the Z-axis RW (the width of each bar-graph is 512 seconds).

flight which would prompt the operators to have closer look at the potential faulty components to determine and investigate the source of a fault. This approach is particularly useful when it is not possible to monitor a large number of low level components continuously.

The purpose of the above performance evaluation has been to determine if the proposed fuzzy rule based reasoning, combined with proposed directed graph-based hierarchical decomposition of the system can achieve acceptable accuracy (close to 95%, as specified in Section 1.4). The results show that it is possible to achieve the desired accuracy by using the proposed HFDM scheme. It is expected that other well known fault diagnosis schemes may achieve similar accuracy in fault identification. However, it is very likely that the other schemes would not address the fault diagnosis problem (as stated in Section 1.4) that is investigated in this thesis. The performance of the traditional ground-based satellite fault diagnosis that is performed via data plotting, trend analysis and limit checking depends heavily on the operator's level of expertise, and there is no standard or universal procedure to perform such analysis. Consequently, a performance comparison of proposed approach with respect to such traditional approaches is not performed in the thesis.

5.5 Advantages and Limitations

A discussion on the advantages and limitations of the proposed methodology is provided below.

Advantages: The proposed hierarchical fault diagnosis model (HFDM) allows one to decompose a complex system systematically in order to perform coherent fault diagnosis. The proposed hierarchical diagnosis algorithm facilitates the identification of the origin of a fault. Fault signatures are represented in the form of fuzzy rules that are transparent and understandable by expert humans. Furthermore, the proposed approach allows integration of fault diagnosis that are performed in various components within a system. The fault dependencies among the components are specified with absolute certainty by using ones and zeros to indicate connectivity/dependency. This simplistic representation of dependencies with link matrices $L_{q,p}^{l_2,l_1}$ helps us to avoid complicated and time demanding model construction. The model allows the incorporation of domain experts' qualitative and imprecise knowledge in the structure of the model as well as in the fuzzy rules that are specified at given node/component, if necessary.

Limitations: The main limitation of the proposed hierarchical fault diagnosis model (HFDM) is that it is possible to specify the dependencies only with absolute certainty by using ones and zeros to indicate connectivity/dependency. Such representation of dependencies may be too simplistic in nature to capture the interaction among various components in the system. Another disadvantage is that once a fault is identified at a component, it is necessary to investigate (as in the proposed *HierarchicalFD* algorithm) rule activations in all the components that are connected to the faulty component (as specified by the associated link matrix) — there is no way to prioritize which components are more probable to be faulty except in cases where a human expert's expertise are available.

5.6 Summary

A hierarchical fault diagnosis methodology that is based on fuzzy rule-based reasoning for satellite formation flight is developed within a novel hierarchical fault diagnosis framework. Fuzzy reasoning-based fault diagnosis is investigated at different levels in the hierarchy for a leader-follower type formation flight of satellites. Intermittent, non-abrupt faults in the attitude control subsystem (ACS) components as well as in the electrical power subsystem (EPS) components with different severity levels have been considered. Fuzzy rules are proposed for identifying faulty components in the satellites formation flight and conditions for fault distinguishability are provided.

The proposed fault diagnosis methodology is demonstrated by utilizing synthetic formation flight data of 5 satellites. The data has been generated via numerical simulations of a satellite formation flight that consists of two subsystems — attitude control subsystem and electrical power subsystem — for each satellite in the formation. Performance evaluation results that correspond to different levels of the hierarchy are also presented. For a given component, performance evaluation was performed by generating a confusion matrix which is a well known and standard procedure for such evaluation. The formation level fault diagnosis is found to be more accurate than the subsystem component level. Consequently, formation level fault diagnosis can be utilized as a supervisory diagnosis system for the formation flight which would prompt the operators to have closer look at the potential faulty components to determine the source of a fault, which is particularly useful when it is not possible to employ continuous monitoring of a large number of low level components. It should be noted there that the performances have not been evaluated in terms of the identification of the fault propagation paths (refer to Section 4.4) because the component dependencies were specified with the link matrix $L_{q,p}^{l_2,l_1}$ (refer to Section 5.2.1) which is simplistic in nature. Such performance evaluation

is left for the next chapter where the dependencies are quantified in terms of conditional probabilities. Finally, advantages and limitations of the proposed method are discussed.

Chapter 6

Bayesian Model-Based Fault Diagnosis

In this chapter Bayesian network-based fault diagnosis is investigated at different levels of the proposed hierarchical decomposition that was presented in Chapter 4.

6.1 Introduction

In Chapter 5, fuzzy rule-based fault diagnosis was investigated at different levels of the proposed hierarchical decomposition that was presented in Chapter 4. A hierarchical fault diagnosis model (HFDM) was developed. In this chapter a Bayesian network-based fault diagnosis model namely, a component dependency model (CDM) is investigated. It is important to recall from the discussions in Chapter 1 that in the case of satellites that operate in near-Earth orbits, it has been possible to manage and operate these systems through additional design margins and extensive ground-based monitoring and control efforts. Fault diagnosis and health monitoring in the Earth orbiting single spacecraft missions are mostly accomplished by human operators at ground through around-the-clock limit-checking and trend analysis on large amount of telemetry data by utilizing software tools. As

explained in chapter 1, this approach does not scale well for multiple space platform missions, and at the same time, it is often desired that expert human operators be involved in the spacecraft operations and diagnosis processes. Therefore, it is desired that the diagnosis model would provide decision support to human experts, and it is reasonable to investigate a Bayesian network (BN)-based (whose capability for human-like reasoning under uncertainties are well-known) fault diagnosis model to relate the faults that are occurring at various subcomponents. This is the rationale behind developing a Bayesian network (BN) type model in the thesis. The proposed Bayesian network-based diagnosis model is generic in the sense that it does not impose any restrictions on the type of diagnosis algorithms that one may employ at a given node of the model as long as its performance evaluation matrix (this is discussed in Section 6.2.3 in detail) is available. In other words, in this chapter we are basically generalizing the HFDM by replacing the link matrices $L_{q,p}^{l_2,l_1}(k', k)$, which were utilized to represent dependency, by some conditional probability tables (CPT) that are commonly used in Bayesian models.

The organization of the remaining parts of this chapter is as follows: In Section 6.2, we start developing a generic BN-based CDM by discussing the scope of the research of this chapter. Next, we discuss the purpose of our model, explain how the health states are defined at different nodes, develop procedure for specifying model parameters, and discuss how evidences are generated at different nodes. In Section 6.3, the proposed scheme is demonstrated by using synthetic data from the formation flight system model that was presented in Chapter 3. The performance evaluation results are presented in Section 6.4, and advantages as well as the limitations of the scheme are discussed in Section 6.5. Finally, the chapter is summarized in Section 6.6.

6.2 Development of a Component Dependency Model (CDM)

It is well-known that elicitation of conditional probabilities for a given Bayesian network-based model is the most difficult aspect of the model development. An overview of the methods that are commonly employed for probability elicitation exhaustively from domain experts is available in [145]. The main drawback of these methods is their biased assessments by experts although various methods for interviewing experts have been developed in literature to reduce such biases. These include probability-scale method [146], gamble-like method [147], and the probability wheel method [148]. Other methods are available in [52] and [53].

The methodology that is presented in this chapter for quantifying the CDM parameters is the result of and is being motivated by the inapplicability of the existing methods (for example, the ones in [52,53]) to the system under consideration in this thesis. Although noisy-OR [55] is a well established method, it applies only to boolean nodes. The method available in [52] utilizes domain-dependent constraints that are not relevant to our problem. The method that is available in [53] is also not applicable because it was developed for ranked nodes whose states are expressed on an ordinal scale which is mapped to a continuous, monotonically ordered, bounded numerical scale. Note that several belief or evidence propagation methods in BN are available in the literature [54,55], and the methods require that the BN parameters of the nodes be specified numerically. Our focus in this chapter is on the BN-based fault diagnosis model development (structure and parameters) as opposed to the development of a belief propagation method.

6.2.1 Objective of the Proposed Bayesian Network Model

First, it is important to describe the main objective of the proposed hierarchical fault diagnosis and health monitoring approach in detail. We intend to utilize this scheme as follows: when the faulty or healthy state of a node is observed by executing a diagnosis algorithm, the evidence (refer to Section 6.2.4 for the specific approach adopted in this thesis) is introduced to our proposed CDM by instantiating that node. The evidence is then propagated in the CDM by utilizing a standard propagation algorithm (such as the *junction tree algorithm* [54,55], *recursive conditioning algorithm* [55], etc.). In the nodes that have updated health states corresponding to the faulty states with high probabilities, diagnosis algorithms are executed to confirm the hypotheses. When a fault evidence is determined at some intermediate level in the hierarchy, the evidence is propagated downwards to identify the component in which the fault has originated from. On the other hand, the evidence is propagated upwards to identify components that are probably affected by the fault, and to determine if higher level specifications are still possible to be accomplished since the diagnosis algorithms at higher levels are usually based on certain rules that check the system (or, system of system) level specifications.

It is possible to encounter situations where there is no identification of a faulty state at a higher level, whereas a low level fault is actually identified at a lower level. However, in such cases, it is worthwhile to propagate the evidence upwards in the hierarchy to identify the high level components that are possibly impacted by the identified fault. On the other hand, when the diagnosis at a higher level is accurate, it is worthwhile to propagate the evidence downwards in the hierarchy to identify the components where one should expect to observe fault manifestations eventhough fault identification cannot be performed at the current instant.

It should be noted that there are certain cost that is associated with performing fault diagnosis at each node in terms of data processing, algorithm development,

validation and performance evaluation. Furthermore, in case of having a large number of components, it is natural from the users' resource considerations that the number of nodes that are to be actively/round the clock monitored is as few as possible. Consequently, it is possible that diagnosis algorithms are not employed at some of the intermediate nodes but it is desired that the nodes be included in the diagnosis model to determine which subsystem or system a faulty node at lower levels belongs to. Such representation allows a systematic fault cause identification.

In subsequent sections, we will investigate a general case of an L level hierarchical decomposition. Before proceeding to the next section it is important to note that the definition of "level l fault" (Definition 4.2.1) plays a significant role in determining the structure of our proposed CDM. Distinguishing faults at different levels based on the above definition allows one to avoid cycles in the CDM.

6.2.2 Proposed Bayesian Network Model Structure and Node States

In this chapter, we represent our proposed hierarchical decomposition with a novel Bayesian network-based Component Dependency Model (CDM) [149] as shown in Figure 6.1. The following notations are consistent with those in Chapters 4 and 5, namely the entire system under consideration is described by a single node at the highest level and which consists of sub-components that are located at lower levels. We denote the p -th component at level l in the hierarchy as C_p^l . For example, if we consider a 4-level decomposition of a fleet of systems as shown in Figure 4.1, for $l = 1$, C_p^1 would correspond to the p -th sensor or actuator (subsystem component) whereas for $l = 4$, C_1^4 would correspond to the "fleet". For the intermediate levels, i.e., $l = 2$ and $l = 3$, a component C_p^l would correspond to the p -th subsystem and system, respectively. Let L denote the total number of levels in the hierarchy, and for any C_p^l , the set of components that are parents of C_p^l (as represented in Figure

6.1) is denoted by $pa(C_p^l)$.

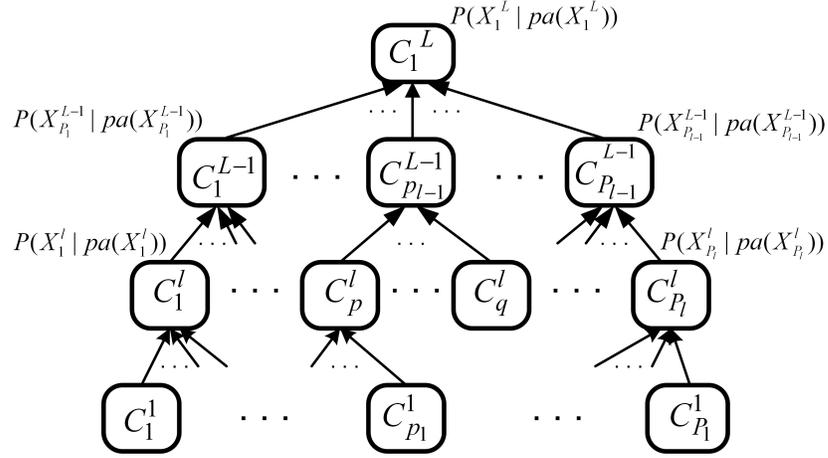


Figure 6.1: Bayesian network representation of an L level hierarchical decomposition.

Node Health States: The possible states of a given node in our proposed CDM represent the health states of the corresponding component. It should be clear, according to the Definition 4.2.1 that the origin of a fault (level l fault) is at one of the nodes C_p^l (refer to Figure 6.1) for which $pa(C_p^l) = \emptyset$. If $pa(C_p^l) \neq \emptyset$, the states of the parent nodes have impact on the states of C_p^l , and the fault may manifest at C_p^l after originating from some other node at lower levels. Depending on whether a node C_p^l has parent nodes or not, we assign its health state as follows: given a component C_p^l and its parents $pa(C_p^l) = \{C_1^{l-1}, \dots, C_m^{l-1}, \dots, C_M^{l-1}\}$, the possible health states X_p^l of C_p^l are represented as $X_p^l = \{x_0, \dots, x_m, \dots, x_M\}$; where x_0 corresponds to the state “healthy C_p^l ” and x_m corresponds to the state “component C_m^{l-1} fault in C_p^l ”. If $pa(C_p^l) = \emptyset$, the possible health states X_p^l of C_p^l are represented as $X_p^l = \{x_0, \dots, x_k, \dots, x_K\}$; where x_k corresponds to the level l fault f_k^l that originates at C_p^l .

Note that it is possible to represent an anomaly in a node that corresponds to multiple simultaneous faults by a health state of the node. However, the diagnosis algorithm that is employed at that node must be capable of distinguishing among

say, two single faults and their simultaneous occurrences. In such a case, from fault identification perspective, the anomaly involving multiple faults can be treated as a “single fault” while generating a node performance evaluation matrix such as a confusion matrix [56]. For sake of simplicity, in this thesis we do not consider health states $x_m \in X_p^l$ (or $x_k \in X_p^l$) that correspond to multiple fault scenarios.

It is worthwhile to note that in Bayesian modeling, it is required that the possible node’s states are exhaustive and mutually exclusive to ensure that the entire state space is under consideration and the node is in a single state at a given instant. These requirements are satisfied in a practical environment by taking into account all the possible, or at least the dominant, faults corresponding to that node that are determined through the well-known Failure Mode Effect and Criticality Analysis (FMECA) procedures.

As mentioned above, node states are observed by executing appropriate fault diagnosis algorithms at that node. Therefore, evidence should be introduced to the network nodes when the states are identified by the diagnosis algorithms without ambiguity. In this chapter fuzzy Rule-Based Reasoning (RBR) (as developed in Chapter 5) is employed to identify the states of a node and to generate evidences (this will be discussed in detail in Section 6.2.4) that are introduced to the node. However, our proposed hierarchical approach is generic for accommodating any type of reasoning algorithm; i.e., at a particular node, Case-Based Reasoning (CBR) or Model-Based Reasoning (MBR) algorithms may be employed as well.

6.2.3 Determination of Model Parameters

Parameters of our proposed Bayesian network-based CDM are the conditional probabilities that are specified in the form of Conditional Probability Tables (CPT). It is well-known that the CPT that is specified at C_p^l has a number of parameters (conditional probabilities) that are exponential in the number of parents $pa(C_p^l)$; i.e., one

must specify $P(X_p^l | pa(X_p^l))$ for each configuration of the parents. An overview of the methods that are commonly employed for probability elicitation from domain experts is available in [145], and the limitations of eliciting probabilities exhaustively with domain experts are well-known. Detailed discussions on the benefits and drawbacks of these methods are available in [145], and reviewing them is therefore beyond the scope of this thesis.

In our case, elicitation of CPTs from the domain expert opinions will be difficult because as the possible number of faults becomes large in the parent nodes of a given node, the number of parent configurations will become too specific for the expert to specify a distribution of the node's health state. Furthermore, it is not reasonable to assume that real data corresponding to different faults and all of their combinations are available. Generating synthetic data for combinations of fault occurrences will be cost prohibitive and challenging, if not impossible, even though a high fidelity simulator is available.

Therefore, a requirement for parameter learning from data is likely to impose a significant barrier in model development and deployment. Furthermore, as mentioned in Section 6.2, the existing methods for generating CPTs are not useful in our case. The above-mentioned difficulties in eliciting probabilities from experts and the unavailability of sufficient data that are always barriers in deploying diagnostic schemes for real systems, have motivated us to investigate alternative methods for generating CPTs.

Uncertainty Information: Recall that our central problem at hand is to manage and utilize the health observations that are available from different subsystems and components. A framework and methodology was proposed in Chapter 4 for system health monitoring where it is desired that diagnostic decisions are made by taking into account the uncertainty that is associated with health state observations at different nodes in the hierarchy. The uncertainty is quantified by the conditional

probabilities that, as indicated above, are commonly elicited by utilizing information from the various sources [150] such as: (a) physical or numerical models, (b) results of experiments or passive observations, and (c) opinions of domain experts.

In the area of health monitoring, the performance metrics for fault detection and identification/isolation are specified separately for both temporal and static performance evaluations [119,151]. Since this chapter is concerned with fault identification by using a probabilistic reasoning model we concentrate on confusion matrices that are used to evaluate static performance of isolation algorithms, and which also provide statistical or probabilistic information.

In the proposed CDM, the health state of a given node is observed by first employing the most appropriate fault diagnosis algorithms that are feasible. Despite the fact that these algorithms are developed by different teams separately and are often proprietary to the teams, it is expected that the diagnosis algorithms that are employed at different nodes have their respective performance evaluation data available, in the form of confusion matrices [56].

A confusion matrix consists of the elements representing the proportion of correct and incorrect classification rates. It is possible to obtain the following conditional probabilities from the confusion matrix that is associated with a given node: $P(X_p^l = x_k | I_p^l = x_n)$; where N is the maximum possible value of k (and n), $k = 0, \dots, N$, $n = 0, \dots, N$, and I_p^l is the health state identification at the node. By utilizing these local conditional probabilities, one can derive the conditional probabilities that are necessary to specify $P(X_p^l | pa(X_p^l))$, and qualify the uncertainty in our proposed CDM as described in the subsequent paragraphs.

Overview of the Proposed Procedure: In [152], it is argued that the care with which any given probability distribution needs to be elicited in a BN model depends strongly on the structure of the model and the queries that are intended to

be processed. The procedure for CPT generation that is proposed in the subsequent paragraphs focuses on a set of initial distributions that are easily verifiable by a human expert. The idea is to construct a set of initial distributions from the information that is available in the confusion matrices, and provide a flexibility to a human expert for modifications, if necessary [149]. There may not be a need for any modification if the expert agrees with the initial distributions. Therefore, instead of asking an expert to provide a new distribution, a procedure is developed to construct distributions that the expert can modify, if necessary, according to his/her belief.

These initial distributions correspond to non-simultaneous sub-component (parent node) faults within a component (child node). Another rationale for providing the non-simultaneous sub-component faults significance is due to the fact that most diagnosis algorithms are designed by incorporating this assumption. Furthermore, it is reasonable to assume that the probability of occurring simultaneous n component faults in a set of components decreases as the number of faults n increases. Once the initial distributions are determined, remaining distributions are derived from these initial ones.

Initial Distributions: Consider a generic segment of our proposed model as shown in Figure 6.2, where the child node C_p^l at level l has N parent nodes at level $l-1$; i.e., $pa(C_p^l) = \{C_1^{l-1}, \dots, C_n^{l-1}, \dots, C_N^{l-1}\}$ and their corresponding number of health states are $(m_1 + 1), \dots, (m_n + 1), \dots, (m_N + 1)$. Consequently, the possible health states of C_p^l are $X_p^l = \{x_0, \dots, x_n, \dots, x_N\}$ and the possible health states of the n -th parent node are $X_n^{l-1} = \{x_i\}; i = 0, 1, \dots, m_n$. In other words, the possible number of parent configurations is $\prod_{n=1}^N (m_n + 1)$. Our objective is to determine a CPT that specifies $P(X_p^l | X_1^{l-1}, \dots, X_N^{l-1})$.

Let I_p^l denote the output of the health state identification algorithm that is employed at the node C_p^l . Hence, the possible outputs of I_p^l correspond to the

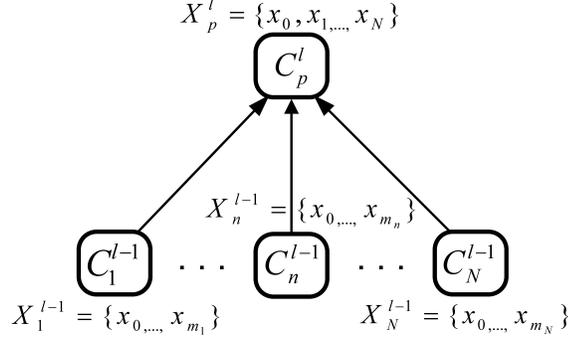


Figure 6.2: Health states of a child node at level l and its parent nodes at level $l-1$.

possible node health states X_p^l ; i.e., $I_p^l = \{x_0, \dots, x_n, \dots, x_N\}$. From the confusion matrix it is possible to obtain the following information: $P(X_p^l = x_k | I_p^l = x_n)$; where, $k = 0, \dots, N$, and $n = 0, \dots, N$. Similarly, at level $l-1$, the information available at the n -th sub-component of C_p^l are: $P(X_n^{l-1} = x_k | I_p^{l-1} = x_i)$; where $k = 0, 1, \dots, m_n$ and $i = 0, 1, \dots, m_n$.

In order to determine the $\prod_{n=1}^N (m_n + 1)$ belief or probability distributions $P(X_p^l | X_1^{l-1}, \dots, X_N^{l-1})$ from the conditional probabilities above, first we focus on the distributions that correspond to single (non-simultaneous) component faults at level $l-1$ and the one that corresponds to the healthy states of all the components at level $l-1$. Our objective is to determine $N_\lambda + 1$ initial distributions over X_p^l , where $N_\lambda = \sum_{j=1}^N m_j$. Note that these distributions correspond to the parent configurations which can be verified relatively easily by a human expert. The N_λ initial distributions that correspond to the fault occurrences at level $l-1$ are in the following general form:

$$P(X_p^l | X_1^{l-1} = x_0, \dots, X_{n-1}^{l-1} = x_0, X_n^{l-1} = x_i, X_{n+1}^{l-1} = x_0, \dots, X_N^{l-1} = x_0) \quad (6.1)$$

where $n = 1, \dots, N$ and $i = 1, \dots, m_n$. The remaining one initial distribution is as

follows:

$$P(X_p^l | X_1^{l-1} = x_0, \dots, X_n^{l-1} = x_0, \dots, X_N^{l-1} = x_0) \quad (6.2)$$

Computation of Initial Distributions: First, it should be noted that there is a systematic pattern by which the health states at level $l - 1$ are mapped to the health states X_p^l at level l in our proposed CDM which is as follows:

Observation 6.2.1 (Health State Mapping). The health states X_p^l of a component at level l and its sub-components at level $l - 1$ are mapped as follows:

- $X_n^{l-1} = x_i; i = 1, \dots, m_n$ are mapped to the state $X_p^l = x_n$ for a given component at level $l - 1$.
- $X_n^{l-1} = x_0; n = 1, \dots, N$ (non-faulty states of multiple components) are mapped to a single state $X_p^l = x_0$.

It is important to note that according to the way node health states are mapped in our modes, and as stated in Observation 6.2.1, $X_p^l = x_0$ is to be considered “true” only when all the parent nodes are healthy; i.e., $X_n^{l-1} = x_0; \forall n$. It is now reasonable to state the following assumption.

Assumption 6.2.1 (Independent Influences of Parent Nodes). Faults or faulty states of the components at level $l - 1$ influence the component health states at level l independently.

Assumption 6.2.1 is particularly valid if the target severity range (refer to the Definition 4.2.1) is low and the components are monitored frequently enough so that the occurrences of faults in one component do not affect the fault identification in other components [143]. Based on this independence assumption, the distribution

in (6.1) is approximated as follows:

$$\begin{aligned}
& P(X_p^l | X_1^{l-1} = x_0, \dots, X_{n-1}^{l-1} = x_0, X_n^{l-1} = x_i, X_{n+1}^{l-1} = x_0, \dots, X_N^{l-1} = x_0) \\
& \approx \left(P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = x), P(X_p^l = x_1 | X_n^{l-1} = x_i), \right. \\
& \quad \dots, P(X_p^l = x_{n-1} | X_n^{l-1} = x_i), P(X_p^l = x_n | X_n^{l-1} = x_i), \\
& \quad \left. P(X_p^l = x_{n+1} | X_n^{l-1} = x_i), \dots, P(X_p^l = x_N | X_n^{l-1} = x_i) \right)
\end{aligned} \tag{6.3}$$

where the first term is conditioned on the health states of all the parent sub-components at level $l - 1$ with $x \neq x_0$ for the n -th sub-component, and $x = x_0$ otherwise. Since $P(X_p^l) = 1$, the distribution in (6.3) is subjected to the constraint

$$\sum_{j=1}^N P(X_p^l = x_j | X_n^{l-1} = x_i) = 1 \tag{6.4}$$

As indicated above, the conditional probabilities that are available from the confusion matrices at levels l and $l - 1$ are local to the nodes at a given level. On the other hand, our problem here is to quantify dependencies between levels l and $l - 1$. The difficulty is that due to different sensitivities of the diagnostic signals at the two levels there is no guarantee that whenever a fault is identified at level $l - 1$ at a given instant, its manifestation at level l is also identified at that instant as well or vice versa.

One way to determine the dependencies is to conduct extensive experiments to observe the relative diagnostic performances of the nodes at the two levels for obtaining each CPT which is quite difficult, if not impossible. Alternatively, according to the way the health state mapping is set up in our model it is easy to see that whenever a faulty state $X_n^{l-1} = x_i$ is identified at level $l - 1$, the component C_p^l becomes faulty (since C_n^{l-1} is a sub-component of C_p^l) — whether the health state of C_p^l is identified as $X_p^l = x_n$ or not. In the case where the fault is not identified at level l , the fault is latent in the sub-component C_n^{l-1} within C_p^l . Based on the above

observations, one can make approximations that if a state at level $l - 1$ is faulty, the state at level l is the corresponding faulty state as well.

Consequently, one can utilize the conditional probabilities that are available from the confusion matrices at level $l - 1$ to specify the distributions in (6.1) and (6.2). Therefore, to practically overcome an unrealistic requirement of conducting extensive experiments, we propose to quantify dependencies by introducing the notion of *hierarchical health state agreement* as follows:

Definition 6.2.1 (Hierarchical Health State Agreement). Given the health state mapping in the Observation 6.2.1, and an identified fault that is manifested as $X_p^l = x_n$, ($n \neq 0$) at level l and $X_n^{l-1} = x_i$, ($i \neq 0$) at level $l - 1$, the health state identifications are in agreement if whenever $I_p^l = x_n$ at level l , $I_n^{l-1} = x_i$, at level $l - 1$.

Based on the Definition 6.2.1, if I_p^l and I_n^{l-1} are known to be in agreement, given $I_n^{l-1} = x_i$, the probabilities of X_p^l and X_n^{l-1} are the same. However, it is necessary to specify the “degree of agreement” to quantify the Definition 6.2.1 in presence of the above-mentioned uncertainties. The following policy is proposed to quantify the degree of agreement by a *belief adjustment factor* that is denoted by $h_{n,i}^{p,n}$ as follows:

$$h_{n,i}^{p,n} = \begin{cases} a_{x_i}^{l-1}/a_{x_n}^l & \text{if } a_{x_i}^{l-1} < a_{x_n}^l \\ a_{x_n}^l/a_{x_i}^{l-1} & \text{if } a_{x_i}^{l-1} > a_{x_n}^l \end{cases} \quad (6.5)$$

where $a_{x_n}^l$ is the accuracy with which the health state x_n is identified at level l . The notion of accuracy is computed by constructing a “one-versus-all” decision matrix (as discussed in [143, 149]) from the confusion matrix by following the procedure that is described next.

Let \mathbf{C}_{con} denote an $(N + 1) \times (N + 1)$ confusion matrix that is associated with $N + 1$ health states of a node at level l in which the actual and the identified health

states are along the rows and the columns, respectively. To compute the accuracy in identifying the n -th state, a 2×2 dimensional “one-versus-all” decision matrix \mathbf{C}_n is constructed as follows. Let $c_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_{con} , and $c'_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_n . The elements of the \mathbf{C}_n matrix are computed from $c'_{2,2} = c_{n,n}$, $c'_{2,1} = (\sum_{k=1}^N c_{n,k}) - c_{n,n}$, $c'_{1,2} = (\sum_{k=1}^N c_{k,n}) - c_{n,n}$, and $c'_{1,1} = (sum(\mathbf{C}_{con}) - c'_{2,2} - c'_{2,1} - c'_{1,1})$. The accuracy of identifying the n -th state is now defined as $a_{x_n}^l = trace(\mathbf{C}_n)/sum(\mathbf{C}_n)$.

Similar procedure is followed to determine $a_{x_i}^{l-1}$. The superscripts p, n in $h_{n,i}^{p,n}$ correspond to the p -th component C_p^l and its n -th health state. The subscripts n, i correspond to the n -th sub-component of C_p^l and its i -th health state. It is important to note that the belief adjustment factor provides one’s degree of belief (in terms of probabilities) about the health states that should be decreased when the level l is changed. Therefore, if the probability of X_n^{l-1} is known given certain condition I , to find the probability of X_p^l given the same condition I , $P(X_n^{l-1}|I)$ should be multiplied by the belief adjustment factor. We consider $(1 - h_{n,i}^{p,n})$ to be a representative of the degree of disagreement.

It is not unusual that in most cases a diagnosis algorithm that is employed at a specific module or component meets the user specified accuracy (say, γ_{spec}) in identifying the component health states by using the test data. For example, in [56], the acceptance criteria for fault isolation/identification given a detection is recommended as $\gamma = 0.95$ in a major component; i.e., the deployed fault identification algorithms should be capable of identifying 95% of the faults that are detected by the fault detection mechanism. Consequently, $\gamma_{spec} \leq a_{x_n}^l \leq 1$, $\gamma_{spec} \leq a_{x_i}^{l-1} \leq 1$, and it follows that $0 < h_{n,i}^{p,n} \leq 1$; where $h_{n,i}^{p,n} = 1$ represents the highest degree of hierarchical agreement.

Note that at any two consecutive levels it is possible to have low accuracies but high belief adjustment factors. Furthermore, it is important to point out that

the above policy is not precise, since as stated in Observation 6.2.1 all the faulty health states of the n -th sub-component at level $l - 1$ are mapped to one health state $X_p^l = x_n$ at level l . Consequently, $a_{x_n}^l$ does not entirely correspond to the health state $X_n^{l-1} = x_i$, ($i \neq 0$). However, it should be clear that with the accuracy $\gamma_{spec} \leq a_{x_i}^{l-1} \leq 1$ in identifying $X_n^{l-1} = x_i$, $i = 1, \dots, m_n$, the policy is expected to be well-behaved. Next, we determine the probability values that are corresponding to the approximated distribution in (6.3) which are categorized into the following three cases:

Case 1: Computation of $P(X_p^l = x_k | X_n^{l-1} = x_i)$ for $k = n$

This is the probability that the state X_p^l is in its n -th faulty state given that the fault has been identified in its n -th subcomponent; i.e., $X_n^{l-1} = x_i$. Since all faulty states of a particular parent node are mapped to a single faulty state of the child node (refer to Observation 6.2.1), as long as the fault is identified at the n -th subcomponent ($X_n^{l-1} \neq x_0$), it is desired that the state at level l be $X_p^l = x_n$. Therefore, one must take into account both the correctly classified faults and the misclassified (with other faults in the subcomponent) faults at level $l - 1$ while computing $P(X_p^l = x_n | X_n^{l-1} = x_i)$.

The probability $P(X_p^l)$ is conditioned on a faulty state which is identified by observing the output of I_n^{l-1} . Therefore, assuming a hierarchical health state agreement (Definition 6.2.1) with the belief adjustment factor $h_{n,i}^{p,n}$, in this thesis we propose the following:

$$\begin{aligned} P(X_p^l = x_n | X_n^{l-1} = x_i) &\approx P(X_p^l = x_n | I_n^{l-1} = x_i) \\ &= h_{n,i}^{p,n} \left(P(X_n^{l-1} = x_i | I_n^{l-1} = x_i) + \sum_{j \neq i, j=1}^{m_n} P(X_n^{l-1} = x_j | I_n^{l-1} = x_i) \right) \end{aligned} \quad (6.6)$$

It may be worthwhile to emphasize that the last term in (6.6) is necessary since when a fault is misclassified as another fault (but not as “healthy”) in a component

at level $l - 1$, the health state of the child component remains the same (faulty).

Case 2: Computation of $P(X_p^l = x_k | X_{1,\dots,N}^{l-1} = x)$ for $k = 0$

The probability $P(X_p^l = x_0 | X_n^{l-1} = x_i)$ is the probability that level l is at a healthy state given that it's n -th sub-component at level $l - 1$ is at a faulty state x_i . Since this is a case of disagreement between the two levels, we use the belief adjustment factor $(1 - h_{n,i}^{p,n})$ in our following computations. Furthermore, since the state $X_p^l = x_0$ is dependent on all the parent sub-components (Observation 6.2.1), we need to take into account the probabilities that are related to all the sub-components' healthy states as follows:

$$\begin{aligned}
& P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = x) \\
& \approx P(X_p^l = x_0 | I_n^{l-1} = x_i) \prod_{j \neq n, j=1}^N P(X_p^l = x_0 | I_j^{l-1} = x_0) \\
& = (1 - h_{n,i}^{p,n}) P(X_n^{l-1} = x_0 | I_n^{l-1} = x_i) \prod_{j \neq n, j=1}^N h_{j,0}^{p,0} P(X_j^{l-1} = x_0 | I_j^{l-1} = x_0)
\end{aligned} \tag{6.7}$$

Case 3: Computation of $P(X_p^l = x_k | X_n^{l-1} = x_i)$ for $k \neq 0$ and $k \neq n$

As in Case 2 above, this is a case of disagreement as well. However, in this case since $k \neq 0$ and $k \neq n$, when the level l is at the state x_k there is no dependency that is represented in the dependency model (Observation 6.2.1) through which x_k can be related to the health state of the n -th sub-component at level $l - 1$. Therefore, the set of probabilities $P(X_p^l = x_k | X_n^{l-1} = x_i)$, $k = 1, \dots, N$ ($k \neq 0$ and $k \neq n$) represent uncertainties that are related to un-modeled dependencies. Given that the distribution in (6.3) has to satisfy the constraint in (6.4), we now propose to distribute beliefs equally among the set:

$$\begin{aligned}
& P(X_p^l = x_k | X_n^{l-1} = x_i) \\
& = \frac{1}{N-1} \left(1 - P(X_p^l = x_n | X_n^{l-1} = x_i) - P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = x) \right)
\end{aligned} \tag{6.8}$$

where $k \neq 0$ and $k \neq n$. The procedure for computing $P(X_p^l = x_n | X_n^{l-1} = x_i)$ and $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = x)$ are described in Case 1 and Case 2, respectively.

Next, in order to determine the distribution in (6.2) we observe that $X_p^l = x_0$ only when all the parent sub-components are healthy. To avoid any ambiguity, we denote the distribution in (6.2) by $P(X_p^l | X_{1,\dots,N}^{l-1} = x_0)$. By Assumption 6.2.1, we now propose to compute the distribution as follows:

$$\begin{aligned}
& P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = x_0) \\
&= 1 - P(X_p^l = \bar{x}_0 | X_{1,\dots,N}^{l-1} = x_0) \\
&= 1 - \prod_{j=1}^N (1 - h_{j,0}^{p,0}) P(X_j^{l-1} = \bar{x}_0 | I_j^{l-1} = x_0)
\end{aligned} \tag{6.9}$$

where \bar{x}_0 corresponds to the set $\{X_p^l\} \setminus x_0$ or $\{X_n^{l-1}\} \setminus x_0$ depending on the level in the hierarchy. The remaining probabilities in the distribution in (6.2), i.e., $P(X_p^l = x_k | X_{1,\dots,N}^{l-1} = x_0)$ where $k = 1, \dots, N$, represent un-modeled dependencies since according to Observation 6.2.1, non-faulty states at level $l-1$ are not mapped to faulty states at level l . In such a situation, as in Case 3 above, we propose to distribute beliefs equally among the set as follows:

$$P(X_p^l = x_k | X_{1,\dots,N}^{l-1} = x_0) = \frac{1}{N} \left(1 - P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = x_0) \right) \tag{6.10}$$

Computation of Initial Distributions When Nodes Are Not Actively Monitored: As mentioned in Section 6.2.2, it may be the case that some nodes in our proposed CDM are not monitored actively. Consequently, fault diagnosis algorithms are not deployed in those nodes. However, since our proposed node health state assignments follow a systematic pattern (refer to Section 6.2.2 and Observation 6.2.1), it is easy to observe that the distributions in (6.1) or (6.3) are expected to be maximum at $X_p^l = x_n$ assuming that the accuracy of the diagnosis algorithm satisfies the user

specification γ_{spec} . Similarly, the distribution in (6.2) is expected to be maximum at $X_p^l = x_0$. Therefore, the initial distributions are specified such that the following conditions are satisfied:

$$\operatorname{argmax}_{x_n \in X_p^l} P(X_p^l | X_{1,\dots,N}^{l-1}) = \begin{cases} x_n & \text{for the distributions in (6.1)} \\ x_0 & \text{for the distribution in (6.2)} \end{cases} \quad (6.11)$$

In order to satisfy the above conditions, in the case of missing information first we assume a near-maximum hierarchical agreement and set $h_{n,i}^{p,n}$ (in (6.6) and (6.7)), and $h_{j,0}^{p,0}$ (in (6.7) and (6.9)) a value that is close to 1. Next, we assume “ideal” probabilities by setting $P(X_n^{l-1} = x_i | I_n^{l-1} = x_i) = \beta_{11}$ (in (6.6)), $P(X_n^{l-1} = x_0 | I_n^{l-1} = x_i) = \beta_{01}$ and $P(X_j^{l-1} = x_0 | I_j^{l-1} = x_0) = \beta_{00}$ (in (6.7)), and $P(X_j^{l-1} = \bar{x}_0 | I_j^{l-1} = x_0) = (1 - \beta_{00})$ (in (6.9)); where $\beta_{11} = \gamma_{spec}$, $\beta_{01} = (1 - \gamma_{spec})$, $\beta_{00} = \gamma_{spec}$, and γ_{spec} is the desired (design specification) probability of the correct health state given an identification in the parent nodes if suitable diagnosis algorithms were employed.

Finally, in the case of a component C_p^{l-1} that does not have a confusion matrix available, but has a similar component C_q^{l-1} with the same health states (for example, the reaction wheel actuators in a three-axis active attitude control subsystem) and a common child node C_p^l , the confusion matrix of C_p^{l-1} may be considered to be the same as that associated with C_q^{l-1} in order to specify the distributions in the CPT at the child node C_p^l . For such a set of similar components, it is also possible to construct a common confusion matrix by including data from the components.

Computation of the Remaining Distributions: Once the initial distributions are determined, we now propose to compute the remaining distributions by using a weighted-sum of the initial distributions, as in (6.1) and (6.2), as follows:

$$P(X_p^l | X_{1,\dots,N}^{l-1}) = \sum_{j=1}^{N_\lambda+1} w_j P_j(X_p^l | X_{1,\dots,N}^{l-1}) \quad (6.12)$$

where $P(X_p^l|X_{1,\dots,N}^{l-1})$ represents $P(X_p^l|X_1^{l-1}, X_2^{l-1}, \dots, X_N^{l-1})$, P_j is an initial distribution, $w_j \in W$, and W is an $(N_\lambda + 1)$ dimensional weight vector that is subjected to the constraint $\sum_{j=1}^{N_\lambda+1} w_j = 1$. It is suggested that the human experts are provided with the initial distributions and are asked to decide the weights w_j based on their judgements. Therefore, given the initial distributions, the proposed procedure would require that the number of weight parameters w_j grows linearly with the total number of the parent nodes' health states.

It is worthwhile to note that as pointed out in [53], it is easy for the human experts to express their opinions in terms of such weight assignments. Therefore, eventhough our procedure is simple, it is consistent with how human experts develop their beliefs by starting from some “anchor” values and adjusting them to specify probabilities (*adjustment and anchoring* heuristics) [153]. Alternatively, one may choose to develop a weight assignment policy that is based on prior probabilities of the faults in the initial distributions under consideration. However, in order to minimize biases towards certain types of faults that are frequently identified, the policy should include other considerations such as component operating hours since some faults may develop only toward the end of life of the component whereas others may develop at the early stages. Development of such a policy is not investigated in this thesis, and has been left as part of the future work.

6.2.4 Evidence Generation

By evidence generation at a node C_p^l with health states $x_k \in X_p^l$, $k = 0, 1, \dots, K$ we refer to the construction of a K dimensional vector $\mathbf{e}_p^l = \{x_0 = 0, \dots, x_k = 1, \dots, x_K = 0\}$ of zeros and ones that is used to instantiate the node when its health state is identified as x_k by employing a suitable fault diagnosis algorithm. As mentioned in Section 6.2.3, component/node health states are identified by employing appropriate/available fault diagnosis algorithms in our CDM nodes. It is possible to obtain

fault evidences by utilizing a fuzzy Rule-Based Reasoning (RBR) method, as developed in Chapter 5, at various nodes of our proposed CDM. The methodology for performing fuzzy RBR at different levels of the hierarchy was presented in our earlier work [143, 154].

It may be recalled from Chapter 5 that it is possible to specify one or more rules for each possible health state $x_k \in X_p^l$ of C_p^l . In the general case, for a given health state x_i and N_d diagnostic signals s_n^l , we synthesize fuzzy rule(s) in the following form (similar to the general if-then rule in Chapter 5):

$$\text{If } (s_1^l \in M_{1,k}^l) \text{ and } (s_2^l \in M_{2,k}^l), \dots, \text{ and } (s_{N_d}^l \in M_{N_d,k}^l) \text{ then } x_k$$

where $x_k \in X_p^l$, and $M_{n,k}^l \in M_p^l$ is a (set of) value(s) of the n -th diagnostic signal (characterized by the fuzzy membership function(s)) when the component health state is x_k . The health state with maximum rule activation level is considered as the identified fault in the node.

It is important to note that the fuzzy rule activation values are not considered as probabilities since they are fundamentally different from each other. As discussed in detail in Chapter 5, if $pa(C_p^l) = \emptyset$, the rules corresponding to the faulty states of C_p^l identify faults that originate in C_p^l with some common and reasonable assumptions in diagnosis, such as non-simultaneous faults within a time step over which the health state of C_p^l is identified and introduced to our proposed CDM.

On the other hand, if $pa(C_p^l) \neq \emptyset$ (as discussed in detail in Chapter 5), the health state of C_p^l is identified by the rules that are synthesized based on the relative behavior specifications of $pa(C_p^l)$ (sub-components of C_p^l) assuming that the interactions of the sub-components are characterized by a leader-follower or master-slave control configuration and ensuring that the master component is in its healthy state before determining the rule activation levels of the slave sub-components.

Once the health state $x_k \in X_p^l$ of C_p^l is identified by employing the above

procedure (or any other reasoning algorithm that is employed at C_p^l) at a given instant, an evidence over the K possible states of C_p^l is generated as follows: $\mathbf{e}_p^l = \{x_0 = 0, \dots, x_k = 1, \dots, x_K = 0\}$, and is subsequently introduced to the C_p^l node of the proposed CDM.

6.3 Demonstration of the Proposed Approach and Fault Diagnosis Results

In a leader-follower formation flight, since the leader acts as a reference point, and the formation flying mission is subjected to a single-point failure of the leader satellite, we propose to reduce the health management workload for only the follower satellites by utilizing our proposed solution. In other words, it is assumed that the leader satellite is healthy as far as our analysis is concerned. This can be ensured if we assume that the components of the leader satellite are monitored and diagnosed frequently enough to ensure that the leader is fault free before carrying out the monitoring and diagnosis of the follower satellites.

Implementation of the Proposed Model: A 4-level Bayesian network-based Component Dependency Model (CDM) has been implemented for the formation flight of 5 satellites that was described in Chapter 3. The open source BN tool that is available from [155] has been utilized for belief propagation and updating using the well-known *recursive conditioning* algorithm [55]. Figure 6.3 shows the implemented CDM where “Sat-1” ... “Sat-5” represent the five satellites in the formation, and “RW-X”, “RW-Y”, and “RW-Z” represent the reaction wheels (RW) in the X , Y , and Z directions, respectively.

First, we assign the states of the components C_p^l with $pa(C_p^l) = \emptyset$ by following the procedure that was described in Section 6.2.2. Each of the 15 RWs, denoted as

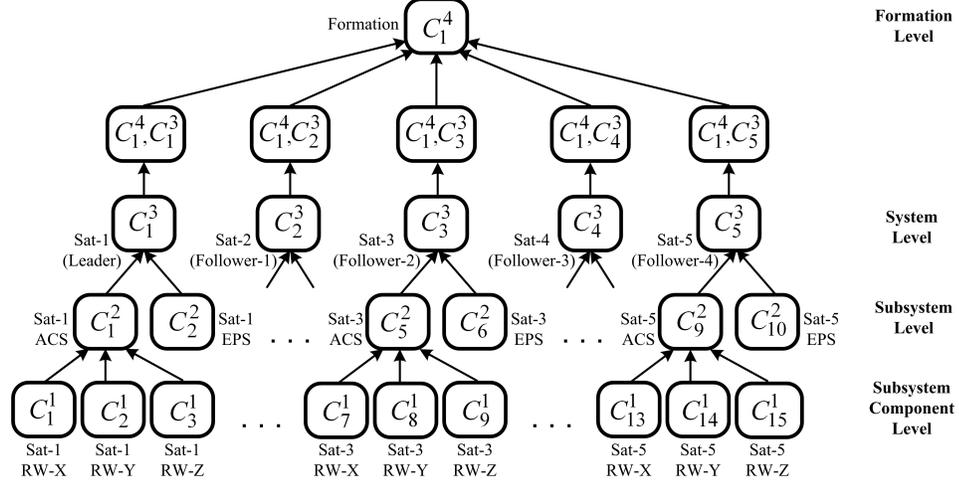


Figure 6.3: A 4-level Bayesian network-based component dependency model (CDM) for hierarchical fault diagnosis.

C_i^1 ; where $i = 1, \dots, 15$ at level 1 (identified as the “subsystem component level”) is assigned with the following 3 health states: $X_i^1 = \{Healthy, friction\ fault, current\ fault\}$ (the fault models are discussed earlier). Each of the 5 electrical power subsystem (EPS) nodes, denoted as C_i^2 ; where $i = 2, 4, 6, 8, 10$ at level 2 (identified as the “subsystem level”) is assigned with the following 3 health states: $X_i^2 = \{Healthy, regulator\ fault, battery\ fault\}$ (the fault models are discussed earlier). We assume that at the beginning of the formation operation, the system is healthy and assign prior probabilities $X_i^1 = \{0.9, 0.05, 0.05\}$; where $i = 1, \dots, 15$, and $X_i^2 = \{0.9, 0.05, 0.05\}$; where $i = 2, 4, 6, 8, 10$, that represent the above assumption.

We assign the states of the components with $pa(C_p^l) \neq \emptyset$ by following the procedure that was specified in Section 6.2.2. Each of the 5 attitude control subsystems (ACS) nodes, denoted as C_i^2 ; where $i = 1, 3, 5, 7, 9$ at level 2 is assigned with the following 4 health states: $X_i^2 = \{Healthy, RW.X\ fault, RW.Y\ fault, RW.Z\ fault\}$. Each of the system level (level 3) nodes or satellites is assigned with the following 3 health states: $X_i^3 = \{Healthy, ACS\ fault, EPS\ fault\}$. In the case of the formation component (C_1^4), note that $|pa(C_1^4)| = 5$ and each parent has 3 states which would lead to a large (3^5) number of parent configurations. Consequently,

first we have implemented 5 intermediate nodes between the levels 3 and 4 which we denote as “ C_1^4, C_i^3 ”; where $i = 1, \dots, 5$. We assign to each of the “ C_1^4, C_i^3 ” nodes 2 states $\{Healthy, Sat.i\ fault\}$. Finally, we assign to the formation component (C_1^4) 3 health states: $X_1^4 = \{Healthy, Leader\ fault, follower\ Fault\}$. Since the health states of the nodes “ C_1^4, C_i^3 ” and C_1^4 are binary, we have implemented a noisy-OR model (as mentioned in Section 6.2) above level 3. In the nodes with $pa(C_p^l) \neq \emptyset$, we specify CPTs by following our proposed procedure in Section 6.2.3.

In the subsequent discussion, we demonstrate how the CPTs in the ACS nodes in Figure 6.3 are specified by using our proposed procedure. Since we are considering identical satellites, we constructed a single confusion matrix for the 15 RWs (C_1^1, \dots, C_{15}^1). Therefore, in this case, the CPTs that are specified in each of the 5 ACS nodes C_i^2 ($i = 1, 3, 5, 7, 9$) are the same. For demonstration purposes and without loss of generality, we consider the ACS of only Sat-1, i.e., the node C_1^2 in the subsequent discussion.

Specification of the CPTs: To specify the CPT node C_1^2 , first note that the parent nodes are three RWs; i.e., $pa(C_1^2) = \{C_1^1, C_2^1, C_3^1\}$. Therefore, the number of parent nodes is $N = 3$. Consequently, the possible number of health states of C_1^2 is $N + 1 = 4$, which are given by $X_1^2 = \{x_0, x_1, x_2, x_3\} = \{Healthy, C_1^1\ fault, C_2^1\ fault, C_3^1\ fault\}$. The possible number of the health states of the parent nodes are $(m_1 + 1) = (m_2 + 1) = (m_3 + 1) = 3$. The possible states of each of the parent nodes, as mentioned above, are $X_i^1 = \{x_0, x_1, x_2\} = \{H, f_f, f_c\}$; where $i = 1, 2, 3$, H represents “Healthy”, f_f represents a “friction fault”, and f_c represents a “current fault”.

The total number of distributions that are required to be specified is $\prod_{n=1}^N (m_n + 1) = 27$. Now, we need to identify the $N_\lambda + 1$ initial distributions over X_1^2 , where $N_\lambda = \sum_{j=1}^N m_j = 6$. The $N_\lambda + 1 = 7$ initial distributions over X_1^2 are given as follows:

- (a) $P(X_1^2|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0)$
- (b) $P(X_1^2|X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_0)$
- (c) $P(X_1^2|X_1^1 = x_2, X_2^1 = x_0, X_3^1 = x_0)$
- (d) $P(X_1^2|X_1^1 = x_0, X_2^1 = x_1, X_3^1 = x_0)$
- (e) $P(X_1^2|X_1^1 = x_0, X_2^1 = x_2, X_3^1 = x_0)$
- (f) $P(X_1^2|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_1)$
- (g) $P(X_1^2|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_2)$

Note that the initial distribution (a) above corresponds to equation (6.2) and the remaining distributions correspond to equation (6.1). To specify the distribution (a) above, we need to compute the following conditional probabilities: (a.1) $P(X_1^2 = x_0|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0)$, (a.2) $P(X_1^2 = x_1|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0)$, (a.3) $P(X_1^2 = x_2|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0)$, and (a.4) $P(X_1^2 = x_3|X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0)$.

Note that we have employed fuzzy rule-based component fault diagnosis (refer to Section 6.2.4) in the following nodes of Figure 6.3 that is the 15 RWs (C_1^1, \dots, C_{15}^1), the five EPSs ($C_2^2, C_4^2, C_6^2, C_8^2, C_{10}^2$), and the formation component (C_1^4). For computing the conditional probability (a.1), we refer to equation (6.9). Since the confusion matrices that are associated with the three parent nodes C_1^1 , C_2^1 , and C_3^1 are the same, the corresponding belief adjustments factor are the same. In addition, since we do not have any diagnosis algorithm deployed in C_1^2 , the information (the values $a_{x_n}^2; n = 0, 1, 2, 3$; refer to the policy that is related to the belief adjustment factor as mentioned in Section 6.2.3) necessary to determine the belief adjustment factor is not available. However, in this case, we have $a_{x_i}^1; i = 0, 1, 2$. We assume $a_{x_n}^2 = 0.95$; for $n = 0, 1, 2, 3$ (close to 1 as mentioned in Section 6.2.3), and from the “one-versus-all” decision matrices (as described in Section 6.2.3) that are obtained from the confusion matrices (associated with the employed rule-based reasoning at nodes C_1^1 , C_2^1 , and C_3^1 , and not shown here), we have, $a_{x_0}^1 = 0.937$, $a_{x_1}^1 = 0.893$, and

$$a_{x_2}^1 = 0.941.$$

Consequently, we have $h_{1,0}^{1,0} = h_{2,0}^{1,0} = h_{3,0}^{1,0} = 0.937/0.95 = 0.986$, $h_{1,1}^{1,1} = h_{2,1}^{1,2} = h_{3,1}^{1,3} = 0.893/0.95 = 0.940$, and $h_{1,2}^{1,1} = h_{2,2}^{1,2} = h_{3,2}^{1,3} = 0.941/0.95 = 0.991$. Since all the parent nodes are associated with the same confusion matrix, as indicated earlier from the confusion matrix we obtain, $P(X_1^1 = \bar{x}_0 | I_1^1 = x_0) = P(X_2^1 = \bar{x}_0 | I_2^1 = x_0) = P(X_3^1 = \bar{x}_0 | I_3^1 = x_0) = 0.071$. With these values, the conditional probability (a.1) is computed as follows: $P(X_1^2 = x_0 | X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0) = 1 - \{(1 - h_{1,0}^{1,0})P(X_1^1 = \bar{x}_0 | I_1^1 = x_0) (1 - h_{2,0}^{1,0})P(X_2^1 = \bar{x}_0 | I_2^1 = x_0) (1 - h_{3,0}^{1,0})P(X_3^1 = \bar{x}_0 | I_3^1 = x_0)\} = 0.999$.

For computing the conditional probabilities (a.2), (a.3), and (a.4) we refer to equation (6.10) and compute the following probabilities: $P(X_1^2 = x_i | X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0) = (1/N) (1 - P(X_1^2 = x_0 | X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0)) = 0.0003$.

Therefore, the initial distribution (a) is computed as $P(X_1^2 | X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_0) = (0.999, 0.0003, 0.0003, 0.0003)$. Next, to specify the distribution (b), we need to compute the following probabilities: (b.1) $P(X_1^2 = x_0 | X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_0)$, (b.2) $P(X_1^2 = x_1 | X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_0)$, (b.3) $P(X_1^2 = x_2 | X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_0)$, and (b.4) $P(X_1^2 = x_3 | X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_0)$.

For computing the conditional probability (b.2), we refer to equation (6.6). The value $P(X_1^1 = x_1 | I_1^1 = x_1) = 0.644$ is obtained from the confusion matrix. Using the value of the belief adjustment factor that was computed earlier as $h_{1,1}^{1,1} = 0.940$, the conditional probability is obtained as follows: $P(X_1^2 = x_1 | X_1^1 = x_1) = h_{1,1}^{1,1} \left(P(X_1^1 = x_1 | I_1^1 = x_1) + P(X_1^1 = x_2 | I_1^1 = x_1) \right) = 0.877$.

For computing (b.1), we refer to equation (6.7) and use the conditional probabilities that are available from the confusion matrix according to the following computations: $P(X_1^2 = x_0 | X_1^1 = x_1) = P(X_1^2 = x_0 | I_1^1 = x_1) \prod_{j=2}^3 P(X_1^2 = x_0 | I_j^1 = x_0) = (1 - h_{1,1}^{1,1})P(X_1^1 = x_0 | I_1^1 = x_1) h_{2,0}^{1,0} P(X_2^1 = x_0 | I_2^1 = x_0) h_{3,0}^{1,0} P(X_3^1 = x_0 | I_3^1 = x_0) = 0.003$.

For computing (b.3) and (b.4), we refer to equation (6.8) and compute the conditional probabilities as follows: $P(X_1^2 = x_k | X_1^1 = x_1) = (N - 1) (1 - P(X_1^2 = x_1 | X_1^1 = x_1) - P(X_1^2 = x_0 | X_1^1 = x_1)) = 0.060$.

Therefore, the initial distribution (b) is obtained as $P(X_1^2 | X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_0) = (0.003, 0.877, 0.060, 0.060)$. By following the same procedure, the initial distribution (c) is computed as $P(X_1^2 | X_1^1 = x_2, X_2^1 = x_0, X_3^1 = x_0) = (0.000, 0.991, 0.0045, 0.0045)$. Now, since we have a single confusion matrix for all the three parent nodes, in this particular case the remaining initial distributions, i.e., (d), (e), (f), and (g) are obtained as $P(X_1^2 | X_1^1 = x_0, X_2^1 = x_1, X_3^1 = x_0) = (0.003, 0.060, 0.877, 0.060)$, $P(X_1^2 | X_1^1 = x_0, X_2^1 = x_2, X_3^1 = x_0) = (0.000, 0.0045, 0.991, 0.0045)$, $P(X_1^2 | X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_1) = (0.003, 0.060, 0.060, 0.877)$, and $P(X_1^2 | X_1^1 = x_0, X_2^1 = x_0, X_3^1 = x_2) = (0.000, 0.0045, 0.0045, 0.991)$, respectively.

The remaining distributions in the CPTs are generated by using equation (6.12). As an example, the distribution associated with two different faults (a “friction fault” in the RW-1 and a “current fault” in the RW-3) is computed by assigning weights (this should be assigned by the human expert) as $P(X_1^2 | X_1^1 = x_1, X_2^1 = x_0, X_3^1 = x_2) = w_2(b) + w_7(g) = (0.0015, 0.4407, 0.0323, 0.5255)$; where $w_2 = 0.5$ and $w_7 = 0.5$ (the two faults are believed to be equally possible), and the remaining weights are set to zero. The computation of the distribution (g) and that of the other distributions are quite similar and are not shown here.

Node Health State Identification and Evidence Generation: In order to generate the health state evidences that are to be introduced at different nodes of our CDM, we have performed a fuzzy rule-based component fault diagnosis (refer to Section 6.2.4) for the following components of Figure 6.3. Specifically, we have the 15 RWs (C_1^1, \dots, C_{15}^1), the five EPSs ($C_2^2, C_4^2, C_6^2, C_8^2, C_{10}^2$), and the formation component (C_1^4).

For the health state identification of the RWs (C_1^1, \dots, C_{15}^1), we have obtained

the diagnostic signals by extracting features from the following reaction wheel (RW) measurements, namely (a) the motor current, (b) the torque command voltage, and (c) the wheel speed. Based on our earlier experience with an actual attitude control subsystem telemetry data [43], we have extracted simple features that include (over an invocation window of 512 seconds; that is approximately 11 invokes per orbit) *mean, standard deviation, minimum value, peak value, energy*, and the first 5 components of the Fast Fourier Transform (FFT) energy spectrum. The rules corresponding to the healthy RW condition as well as to the two faults under consideration are determined (the general form of the rules is given in equation (5.1) and the details are available in [143] and are not discussed here), and the rule activations in each invocation are computed.

Similarly, to identify the health states of the EPSs ($C_2^2, C_4^2, C_6^2, C_8^2, C_{10}^2$), we have obtained the diagnostic signals by extracting features from the following EPS measurements, namely (a) the bus voltage, (b) the regulator output current, and (c) the battery current. We have extracted simple features that include (over the above-mentioned invocation window of 512 seconds) *mean, standard deviation, minimum value*, and the one component of the Fast Fourier Transform (FFT) energy spectrum. Rules corresponding to the healthy EPS condition as well as to the two faults under consideration are determined by utilizing the above features.

For the health state identification of the formation (C_1^4), *mean of the relative attitude measurements* over an invocation window is utilized as a diagnostic signal. As in the case of RWs, the rule activations in each invocation are computed for EPSs and for the formation level. Note that the health state evidences corresponding to the formation node are introduced at the intermediate nodes as mentioned earlier.

Hierarchical Diagnosis: At this stage fault evidences at different levels to the CDM are introduced, the evidences are propagated, and belief distributions of the CDM nodes are updated by using the well-known *recursive conditioning* algorithm

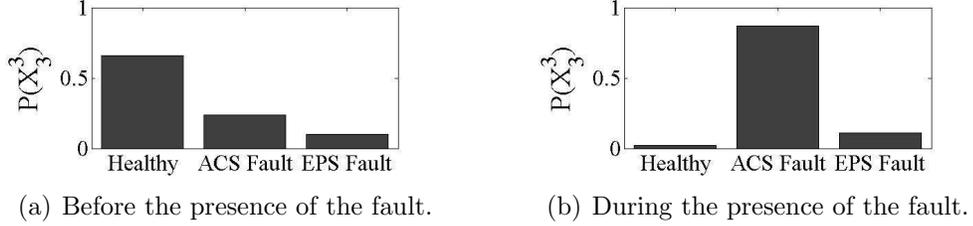


Figure 6.4: $P(X_3^3)$ of Sat-3 when an evidence of a fault is introduced at the subsystem component level.

[55]. In most cases, the computed distributions clearly justified the existence of faults. For example, when the fault evidence $\mathbf{e}_9^1 = \{0, 1, 0\}$ (friction fault at Sat-3 RW-Z) is introduced, the probability distributions over the health states of Sat-3 under the fault free condition as well as under the injected friction fault at Sat-3 RW-Z are shown in Figure 6.4. The distributions clearly justify the existence of a fault in the ACS. The distributions corresponding to the other fault scenarios are not graphically presented here. Instead, the accuracy of the hierarchical fault diagnosis results are summarized under various scenarios in the next section.

6.4 Performance Evaluation

We evaluate the performance of our proposed CDM by using a set of fault scenarios under which the actual health states of all the nodes in the CDM are known. The accuracy is computed in terms of the % of nodes in the CDM that are “representative” of their true known health states. The representativeness is determined as follows: let a fault evidence $\mathbf{e}_{p_1}^{l_1}$ be introduced at node $C_{p_1}^{l_1}$ and the known actual health state of a component $C_{p_2}^{l_2}$ be $x^* \in X_{p_2}^{l_2}$. Furthermore, let $\pi(C_{p_1}^{l_1})$ and $\sigma(C_{p_1}^{l_1})$ denote the sets of predecessors and successors of node $C_{p_1}^{l_1}$, respectively in the CDM. We consider the health state of $C_{p_2}^{l_2}$ to be *representative* of its true health state x^* when the following specifications or conditions hold:

1. Let $C_{p_2}^{l_2} \in \sigma(C_{p_1}^{l_1})$, then belief about $X_{p_2}^{l_2} = x^*$ increases with the introduction

of the evidence; i.e., $P(X_{p_2}^{l_2} = x^* | \mathbf{e}_{p_1}^{l_1}) > P(X_{p_2}^{l_2} = x^* | \emptyset)$.

2. Let $C_{p_2}^{l_2} \in \pi(C_{p_1}^{l_1})$ and the actual known state be faulty ($x^* \neq x_0$), then belief about $X_{p_2}^{l_2} = x^*$ increases with the introduction of the evidence, and the belief is higher than (or, at least equal to) that of other fault states at level l_2 ; i.e., $P(X_{p_2}^{l_2} = x^* | \mathbf{e}_{p_1}^{l_1}) > P(X_{p_2}^{l_2} = x^* | \emptyset)$ and $P(X_{p_2}^{l_2} = x^* | \mathbf{e}_{p_1}^{l_1}) \geq P(X_p^{l_2} = x_j | \mathbf{e}_{p_1}^{l_1})$; where $x_j \neq x_0$, $x_j \neq x^*$ and p represents the component at level l_2 at which no evidence has been introduced.
3. Let $C_{p_2}^{l_2} \in \pi(C_{p_1}^{l_1})$ and the actual known state be healthy ($x^* = x_0$), then the belief about the faults in $C_{p_2}^{l_2}$ are lower than that in the faulty components at level l_2 ; i.e., $P(X_{p_2}^{l_2} = x | \mathbf{e}_{p_1}^{l_1}) < P(X_p^{l_2} = x_j | \mathbf{e}_{p_1}^{l_1})$; where $x \in \{X_{p_2}^{l_2} \setminus x^*\}$, $x_j \neq x_0$ and p represents the faulty component, if any, at level l_2 at which no evidence has been introduced.

If there is no known faulty component at level l_2 (fault originated at $C_{p_3}^{l_3}$, $l_1 < l_3 < l_2$), then the belief distribution over $X_{p_2}^{l_2}$ is maximum at x^* and $P(X_{p_2}^{l_2} = x | \mathbf{e}_{p_1}^{l_1}) < P(X_{p_3}^{l_3} = x_j | \mathbf{e}_{p_1}^{l_1})$; where $x \in \{X_{p_2}^{l_2} \setminus x^*\}$ and $x_j \neq x_0$.

4. Let $C_{p_2}^{l_2} \notin \{\pi(C_{p_1}^{l_1}) \cup \sigma(C_{p_1}^{l_1})\}$, then the belief distribution over $X_{p_2}^{l_2}$ remains unchanged with the introduction of the evidence; i.e., $P(X_{p_2}^{l_2} | \mathbf{e}_{p_1}^{l_1}) = P(X_{p_2}^{l_2} | \emptyset)$.

It is obvious that given a fault evidence at a node, when the CDM node states are representative of their true known health states as per the condition stated above, the fault propagation path(s) (refer to Section 4.4) is/are identified. In other words, a path is formed with a set nodes at which probability of the fault state (corresponding to the introduced evidence) becomes higher when the evidence is introduced at the node.

Table 6.1 shows the computed accuracy under various scenarios with single as well as multiple fault evidences that are introduced in the follower satellites in the CDM as shown in Figure 6.3. By “conflicting” evidence in Table 6.1 it is implied that

Table 6.1: Performance Evaluation of the Implemented CDM

Number of Evidences	Number of Scenarios	Maximum Accuracy (in % Nodes)	Minimum Accuracy (in % Nodes)	Average Accuracy (in % Nodes)	Comments
Single Fault in a Follower Satellite					
1	16	100%	83.33%	97.91%	None
2	20	100%	100%	100%	Evidences introduced at different levels
2	8	91.67%	86.11%	90.28%	Conflicting evidence at levels 1 or 2
2	8	100%	100%	100%	Conflicting evidence at formation level
Two Simultaneous Faults in Two Follower Satellites					
2, 3, 4	72	100%	77.78%	90.43%	Different evidence types and combinations

for the two evidences that are available in two nodes connected through a directed path, one evidence indicates a healthy state while the other indicates a faulty state. Such a scenario is possible when, for example, a fault evidence in a node at the high level is obtained but at the low level the fault is not identified or vice-versa.

Note that although the scenarios are not the only possible cases, they represent some of the most common cases that may occur in practice. The average accuracy is computed over all the scenarios under consideration. Row 1 represents scenarios where a single fault evidence is introduced at a given node and the accuracy is computed for each scenario (by using the conditions above). It is observed that when one additional evidence is introduced (refer to row 2), the average accuracy increases. However, if the additional evidence is conflicting and the mis-identification is at the low level, the average accuracy decreases (refer to row 3). Furthermore, if the additional evidence is conflicting but the mis-identification is at the high level, the accuracies remain unchanged (refer to row 4). Finally, the last row shows accuracies for two simultaneous faults in two different follower satellites where the scenarios consist of both conflicting and non-conflicting evidences.

The purpose of the above performance evaluation has been to determine if the proposed CDM can achieve acceptable accuracy (close to 95%, as specified in Section 1.4). The results show that it is possible to achieve the desired accuracy by using the proposed CDM scheme. It is expected that other well known fault diagnosis schemes may achieve similar accuracy in fault identification. However, it is very likely that the other schemes would not address the fault diagnosis problem (as stated in Section 1.4) that is investigated in this thesis. As mentioned before, the performance of the traditional ground-based satellite fault diagnosis that is performed via data plotting, trend analysis and limit checking depends heavily on the operator’s level of expertise, and there is no standard or universal procedure to perform such analysis. Consequently, a performance comparison of proposed approach with respect to such traditional approaches is not performed in the thesis.

6.5 Advantages and Limitations

As in any large Bayesian network model, building a BN-based hierarchical fault diagnosis model as proposed in this thesis involves a careful trade-off between a rich hand-crafted model versus generic dependency model. The design considerations to take into account are model parameters and result accuracies, the cost of construction (including the demand for human experts’ time), maintenance (including the cost of model updating), and the complexity of the probabilistic inference. Consequently, in practice, building such a model requires multiple iterations over these tasks until a satisfactory model and solution is achieved. A discussion on the advantages and limitations of the proposed methodology is provided below.

Advantages and Comparison with HFDM: First it should be noted that the proposed component dependency model (CDM) is a generic model that can be used to decompose a complex system hierarchically in order to perform coherent

fault diagnosis. The model is generic in the sense that (a) the health states of a given component is not defined subjectively, rather they are identified by the known dominant fault modes of the component, and (b) the proposed method does not impose any restrictions on the type of diagnosis algorithms that one may employ at a given node of the model as long as its performance evaluation matrix is available. Furthermore, our proposed method for obtaining model parameters overcomes the limitations of the other probability elicitation methods [52, 53, 145] as discussed in Section 6.2.3.

Second, the proposed approach requires less demand on domain experts' time for obtaining the model parameters, which is known to be a costly commodity. Instead of entirely depending on interviewing domain experts, the initial distributions are obtained from node fault diagnosis performance data and known health state dependencies. This minimizes the well-known limitations of eliciting probabilities exhaustively with domain experts.

Third, the model parameters are easy to update when node performance matrix changes due to the availability of new data and improved versions of the node fault diagnosis algorithm. In this case, the initial distributions can be re-computed by following our proposed well-defined procedure (this avoids the repetition of the time consuming interview of domain experts), and the weights, if necessary, may be updated.

Finally, for formation flight fault diagnosis, the proposed CDM enables one to hierarchically decompose a complex system in order to use the data that are available from different system components systematically, and to perform diagnostic reasoning coherently. By propagating fault evidences from a node in the CDM, one is able to update the probable health state of the other nodes, and perform in-depth investigation of the nodes of interest only (based on the updated health states). This avoids exhaustive plotting and trend analysis across a large number of components

manually which requires extensive effort by human operators. Therefore, the approach has the potential for reducing the size of the operations team. Furthermore, since the performance evaluation matrix data represents an expert human's observations to a great extent, and the method obtains model parameters by utilizing such matrices, less-experienced personnel will be benefited while performing monitoring and diagnosis tasks at ground stations by utilizing our proposed model.

Note that there will always be a trade-off between a rich/detailed hand-crafted model versus a generic dependency model. It is clear from the above discussion that our proposed model will reduce the cost of model construction (the demand for human experts' time) and maintenance (the cost of model updating).

With the HFDM approach that was developed in Chapter 5, it was possible to specify the dependencies only with absolute certainty by using ones and zeros to indicate connectivity/dependency as opposed to using BN-based models and CPTs. Consequently, if a fault evidence is found at a given node, fuzzy rule activations had to be computed at all the parent nodes, and it was not possible to propagate beliefs to update and estimate health states without computing the rule activations. Given the fault evidence(s) and updated belief distributions, in this chapter we compute the rule activations at only those nodes that have high fault probabilities to confirm the identification of a fault.

Limitations: The main limitation of the proposed method is that the faults that originate in a component at a particular level are implicitly assumed to be non-interfering with the diagnostic signals of other components (that have a common child node) at the same level. This assumption is reasonable when the fault diagnosis algorithms that are deployed in those nodes are designed to identify faults with a severity range that is low enough not to affect the performances of the other nodes in the same level. Consequently, their influences on the child nodes are to be considered as independent. Note that this limitation arises from the type of

information that is made available to the proposed model development. Specifically, according to our problem in hand, the node fault diagnosis algorithms are developed in isolation, and are often proprietary to the development teams. Nevertheless, one should investigate the validity of the independence assumptions by using design information and experimental data. Another limitation may be the *belief adjustment factor* that is denoted by $h_{n,i}^{p,n}$ in equation (6.5). The policy may be too simple for some systems.

6.6 Summary

In this chapter, a hierarchical fault diagnosis methodology was developed which allows systematic and coherent fault diagnosis in different components or subsystems of a complex formation flight of satellites. The general idea is to decompose a complex system hierarchically into simpler modules or nodes, and perform diagnostic reasoning hierarchically by utilizing the fault diagnosis algorithms that are deployed at different nodes and which are connected via the proposed Bayesian network-based Component Dependency Model (CDM). The model structure was developed from the knowledge of the component health state dependencies. A methodology for determining model parameters was developed which demands considerably less effort from the domain experts, and easy to update when node fault diagnosis performances change. To determine the probability distributions that are required and that need to be specified in the Conditional Probability Tables (CPT), the proposed method obtains certain initial probability distributions from the node fault diagnosis performance matrices. Subsequently, by taking the domain experts' opinion into account, the remaining probability distributions are specified.

The effectiveness of our proposed methodology has been demonstrated by utilizing synthetic formation flight data of 5 satellites that was described in Chapter 3.

As mentioned in Chapter 3, the data generation model consists of two subsystems, namely the attitude control subsystem and the electrical power subsystem for each satellite in the formation. The proposed CDM was implemented by decomposing the formation flying system hierarchically into 4 levels. Fault evidences that are generated via fuzzy rule-based reasoning of faults at different levels in the hierarchy were introduced in the CDM nodes. The fault diagnosis results show that when fault evidences are introduced at a node, the states of the remaining nodes of the implemented CDM are updated to reflect the correct health states of the corresponding components. The performance of the developed CDM was quantified which corresponds to the identification of fault propagation path that was defined in Chapter 4. In the next chapter, verification and validation of the fault diagnosis models that have been proposed in this thesis are investigated.

Chapter 7

V&V of Hierarchical Fault Diagnosis

In this chapter, the verification and validation (V&V) of the Bayesian network-based fault diagnosis model namely, CDM that was developed in Chapter 6 is primarily investigated. The V&V of the fuzzy rule-based fault diagnosis model namely, HFDM that was developed in Chapter 5 is also briefly discussed.

7.1 Introduction

V&V of artificial intelligence models and algorithms is a challenging area where quite limited research have been pursued [156–159]. Validation ensures that a product (in this thesis, a model) actually meets the user’s needs, and that the specifications were correct in the first place, while verification ensures that the product has been built according to the requirements and design specifications.

In this thesis, the term “V&V of a fault diagnosis model” implies that the verification of the model does satisfy a generic requirement, namely that “the model shall be capable of identifying the health states of the system under consideration”. Furthermore, V&V of the hierarchical fault diagnosis is divided into two levels: (1)

the overall model level, and (2) the node level. The former is related to the problem of the V&V of Bayesian knowledge bases. The later is dependent on what type of algorithm is deployed at a given node. In our case, this investigation is related to the V&V of fuzzy rule bases since fuzzy rule-based reasoning is employed at different nodes of the implemented CDM and HFDM.

Formal verification of fuzzy rule bases are usually performed by utilizing petri-net models to ensure that certain properties of rules in the rule base are satisfied. Such rule base V&V approaches have already been investigated in the literature to a large extent [160]. However, there has been very few published work [150,161–163] on the verification of Bayesian knowledge bases.

The overall fault diagnosis algorithm development and V&V process that is proposed in this thesis is depicted in Figure 7.1. which essentially summarizes the

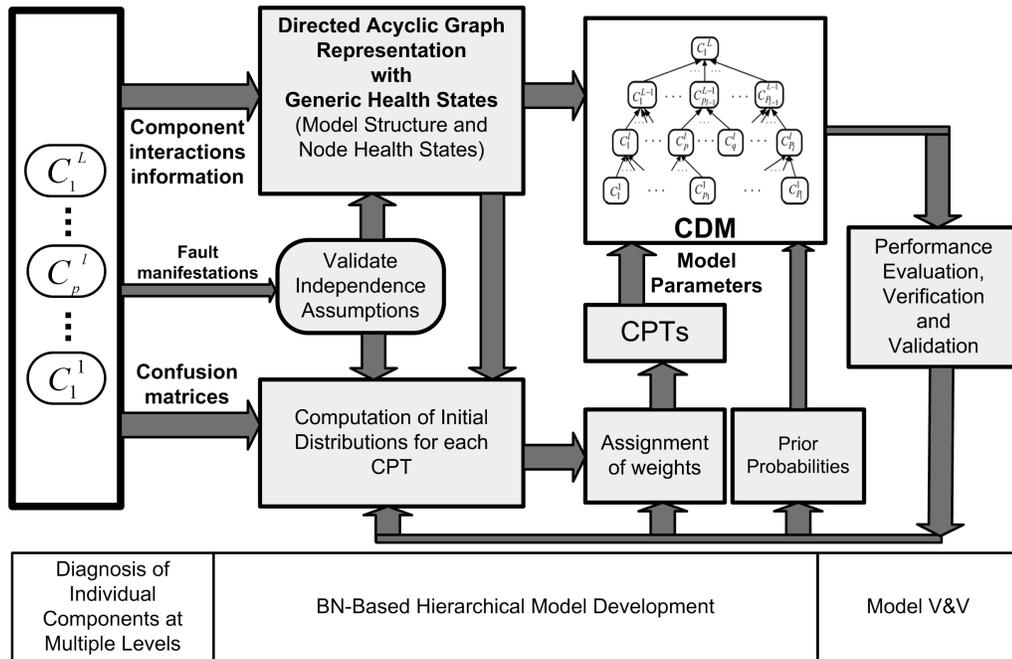


Figure 7.1: Development and validation process of the proposed fault diagnosis models.

fault diagnosis model development process that was discussed in Chapter 6, and adds the V&V of the model with the process. In Figure 7.1, the overall process is

divided into three stages: (1) diagnosis of individual components at multiple levels, (2) BN-based hierarchical model development, and (3) model V&V. Note that at stage 2, it is necessary to validate independent assumptions that are made while determining the model structure or node conductivities (as mentioned in Section 6.5). Such validation should be performed at early stage in order to avoid major changes in the model at the “model V&V” stage where ideally only model parameter tuning should take place. In this thesis, it was assumed that the model structure and the component interactions are known for the given formation flight model, and such direct validation of the independence assumption is considered to be beyond the scope of the thesis.

It is evident from Chapters 5 and 6 that fuzzy rule base reasoning can be employed at the first stage, namely “diagnosis of individual components at multiple levels” of CDM development. In that case, the verification of fuzzy rule base can be performed at each node/component separately, whereas the V&V of the CDM corresponds to the overall model and takes into account interaction of various nodes in the model.

In the subsequent sections first, the verification of the Bayesian network-based fault diagnosis model namely CDM that was developed in Chapter 6 is investigated in detail. Next, the V&V of the fuzzy rule-based fault diagnosis model namely HFDM that was developed in Chapter 5 is briefly discussed.

7.2 Development of a Verification Approach for CDM

Sensitivity analysis (SA) is a well-known and standard method for verifying Bayesian networks which allows systematic investigation of influences of the model parameters on its outputs. The general objective of the sensitivity analysis is to investigate

how one or more hypothesis variables in a network varies with the variation of one or more parameters (a parameter is an entry in a conditional probability table (CPT)) in the network. Sensitivity analysis helps one to ensure that the constructed Bayesian network is not too sensitive to small variations in network parameters. A brute-force method for varying the parameters involves the variation of every single conditional probability, and such sensitivity analysis is both highly time-consuming and computationally intensive process. Therefore, a systematic SA approach is required for the V&V of a Bayesian network model.

As reviewed in Section 2.2.3, the most common approach for sensitivity analysis assumes *proportional scaling*. Under this assumption, if X has n states, and x_1 is a parameterized state, it is assumed that $P(X|\pi) = (t, (1-t)x_2, \dots, (1-t)x_n)$, where $\sum_{i=1}^n x_i = 1$. It is possible to deal with several parameters in the same distribution. If, for example, the first two states are parameterized, one would require $P(X|\pi) = (t, s, (1-t-s)x_3, \dots, (1-t-s)x_n)$. Then, s does not scale when t is changed. By varying a (set of) network parameters in the above-mentioned approach one is interested to know how $P(h|e)$ varies with the parameter variation; where H is a hypothesis variable and h is a particular state of H which is the focus of interest.

The above method for varying the network parameters is primarily useful in situations when one is interested to investigate the sensitivity of the network output due to a change in parameter(s) that is caused by probability elicitation (from domain experts) error. However, in the component dependency model (CDM) that is proposed in Chapter 6, the conditional probabilities are obtained from confusion matrices. Therefore, one must investigate how a change in a confusion matrix impacts the network performance. Therefore, *the objective here is to investigate how a change in the fault diagnosis performance at a given node affects the network outputs.*

In other words, our objective is to perform the verification that the CDM satisfies a more specific requirement, namely that “the model shall be negligibly sensitive to small changes in its parameters” (this requirement is clearly related to the generic requirement that was stated in Section 7.1). The term “negligibly” is however somewhat subjective here which can be clarified by quantifying it in terms of the changes in probability values, if necessary.

It is not difficult to realize that the above procedure which assumes *proportional scaling* is not suitable for the component dependency model (CDM) that is proposed in Chapter 6. This is due to the fact that a change in a confusion matrix impacts the computation of initial probability distributions (as proposed in Section 6.2.3) – and consequently, almost the entire CPT – in a way that does not satisfy the proportional scaling assumption. In the subsequent sections, a sensitivity analysis procedure for the proposed CDM will be investigated. The investigation is divided into two parts: (a) the analysis of parameter variation in CDM, and (b) the proposed verification steps.

7.2.1 Parameter Variation in the CDM

First, we investigate how the parameters in the proposed CDM are varied due to a change in the associated confusion matrix. In other words, we will consider a specific change in a confusion matrix that corresponds to a fault mode identification at a node of the CDM, and investigate how this change would affect the CDM parameters. We consider a general case of such parameter variation which is investigated in the subsequent paragraphs.

Let C_p^l be a node in the CDM, and $C_1^{l-1}, \dots, C_N^{l-1}$ are the parent nodes of C_p^l . According to the notations in Chapter 6, the states of $X_p^l = x_0, x_1, \dots, x_n, \dots, x_N$; $x_n \neq x_0$ correspond to the faulty subcomponents of C_p^l and x_0 corresponds to the state of C_p^l when all the subcomponents of C_p^l are healthy. For the sake of convenience

Table 7.1: The Change in the Confusion Matrix at the Node C_1^{l-1} Caused Due to a Change of the Performance of the Diagnosis Algorithm Deployed at the Node

Identified \rightarrow Actual \downarrow	f_0	f_1	f_2	...	f_{K_1}
f_0	$c_{0,0}$	$c_{0,1}$	$c_{0,2}$...	c_{0,K_1}
f_1	$c_{1,0} + \rho_0\delta$	$c_{1,1} - \delta$	$c_{1,2} + \rho_2\delta$...	$c_{1,K_1} + \rho_{K_1}\delta$
f_2	$c_{2,0}$	$c_{2,1}$	$c_{2,2}$...	c_{2,K_1}
...
f_{K_1}	$c_{K_1,0}$	$c_{K_1,1}$	$c_{K_1,2}$...	c_{K_1,K_1}

in notation, and without loss of generality, let us assume that the states of the n -th parent node are $X_n^{l-1} = f_0, f_1, \dots, f_k, \dots, f_{K_n}$, where $f_k \neq f_0$ corresponds to the faults in C_n^{l-1} and f_0 corresponds to the healthy state of the node.

Without any loss of generality, we consider a change in the confusion matrix of C_1^{l-1} that corresponds to the identification of the first fault mode f_1 in C_1^{l-1} . Specifically, let us consider the change in the confusion matrix of C_1^{l-1} which is caused due to a change of performance of the diagnosis algorithm deployed at the node, as shown in Table 7.1. Note that prior to the change in $c_{1,1}$ number of cases the fault mode or state f_1 was identified correctly as shown in Table 7.1. Now, due to the change in performance of the diagnosis algorithm that is deployed in C_1^{l-1} , the number reduces to $c_{1,1} - \delta$. This implies that in the δ number of cases the faulty state f_1 is now misidentified as other states of the node which are represented in terms of $\rho_k\delta$, where $k = 0, \dots, K_1, k \neq 1$ and $\sum_{k \neq 1, k=0}^{K_1} \rho_k = 1$. We denote the parameter of our interest by $\theta = P(X_1^{l-1} = f_1 | I_1^{l-1} = f_1)$ which signifies the probability of C_1^{l-1} being in its state $X_1^{l-1} = f_1$ given an identification f_1 by the diagnosis algorithm deployed at C_1^{l-1} . In terms of the changed confusion matrix elements in Table 7.1, the parameter of our interest is $\theta = (c_{1,1} - \delta) / ((\sum_{j=0}^{K_1} c_{j,1}) - \delta)$.

Recall from the CDM parameter computation procedure that was proposed in Section 6.2.3, the above change in the confusion matrix of C_1^{l-1} will impact the CDM parameters (the entries of the CPT) that are stored in C_p^l . Since the CPT is

computed from the initial distributions, one first need to identify how the change impacts the initial distributions. Therefore, the changes in the following general cases of the $N_\lambda + 1$ (in this case, $N_\lambda = \sum_{n=1}^N K_n$, as explained in Section 6.2.3) initial distributions over X_p^l require attention, specifically for:

Case 1: $P(X_p^l | X_1^{l-1} = f_1, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0)$

Case 2: $P(X_p^l | X_1^{l-1} = f_k, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0)$, where $k = 2, \dots, K_1$

Case 3: $P(X_p^l | X_1^{l-1} = f_0, \dots, X_n^{l-1} = f_k, \dots, X_N^{l-1} = f_0)$, where $n = 2, \dots, N$ and $k = 1, \dots, K_n$

Case 4: $P(X_p^l | X_1^{l-1} = f_0, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0)$

To investigate the above initial distributions the following results are required.

Proposition 7.2.1 (Accuracy Change). Let the change in the confusion matrix of a node C_1^{l-1} , caused due to a change of performance of the diagnosis algorithm deployed at the node, is according to Table 7.1. Let $\theta = (c_{1,1} - \delta) / ((\sum_{j=0}^{K_1} c_{j,1}) - \delta)$. Then, the accuracy of identifying the faulty state f_1 can be expressed according to $a_{f_1}^{l-1} = a_1\theta + b_1$, where a_1 and b_1 are real-valued numbers.

Proof. Recall that for computing hierarchical agreement factors in Chapter 6, the accuracy $a_{f_1}^{l-1}$ (with which the health state f_1 is identified at level $l-1$) is computed by constructing a 2×2 dimensional “one-versus-all” decision matrix \mathbf{C}_1 (as discussed in Section 6.2.2). Let \mathbf{C}_{con} denote an $(K_1 + 1) \times (K_1 + 1)$ confusion matrix that is associated with $K_1 + 1$ health states of the node C_1^{l-1} as shown in Table 7.1. Let $c_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_{con} , and $c'_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_1 . The elements of the \mathbf{C}_1 matrix are computed as follows:

$$\begin{aligned} c'_{2,2} &= c_{1,1} - \delta \\ c'_{2,1} &= \left(\sum_{k=0}^{K_1} (c_{1,k} + \rho_k \delta) \right) - (c_{1,1} - \delta) \\ &= \left(\sum_{k \neq 1, k=0}^{K_1} (c_{1,k} + \rho_k \delta) \right) + (c_{1,1} - \delta) - (c_{1,1} - \delta) \end{aligned}$$

$$\begin{aligned}
&= \left(\sum_{k \neq 1, k=0}^{K_1} c_{1,k} \right) + \delta = \kappa_{21} + \delta; \text{ since } \sum_{k \neq 1, k=0}^{K_n} \rho_k = 1 \\
c'_{1,2} &= \sum_{k \neq 1, k=0}^{K_1} c_{1,k} = \kappa_{12} \\
c'_{1,1} &= \text{sum}(\mathbf{C}_{con}) - c'_{2,2} - c'_{2,1} - c'_{1,1} = \kappa_{11}
\end{aligned}$$

where $\kappa_{21} = (\sum_{k \neq 1, k=0}^{K_1} c_{1,k})$, $\kappa_{12} = (\sum_{k \neq 1, k=0}^{K_1} c_{1,k})$, and κ_{11} are real numbers that are independent of δ and ρ_k s. Furthermore, $\rho_1 = 1$ as per Table 7.1.

The accuracy of identifying the 1-st fault state is computed as follows:

$$\begin{aligned}
a_{f_1}^{l-1} &= \text{trace}(\mathbf{C}_1) / \text{sum}(\mathbf{C}_1) \\
&= (c_{1,1} - \delta + \kappa_{11}) / (c_{1,1} + \kappa_{11} + \kappa_{12} + \kappa_{21}) \\
&= \kappa(c_{1,1} - \delta) + \kappa\kappa_{11}
\end{aligned}$$

where $\kappa = 1 / (c_{1,1} + \kappa_{11} + \kappa_{12} + \kappa_{21})$. Dividing and multiplying the first term by $(\sum_{k=0}^{K_1} c_{k,1}) - \delta$, and approximating for a small change δ the term $\kappa((\sum_{k=0}^{K_1} c_{k,1}) - \delta) \approx \kappa(\sum_{k=0}^{K_1} c_{k,1})$, the accuracy can be expressed in the form:

$$a_{f_1}^{l-1} = a_1\theta + b_1$$

where $a_1 = \kappa(\sum_{k=0}^{K_1} c_{k,1})$ and $b_1 = \kappa\kappa_{11}$ are real numbers that are independent of δ and ρ_k . \square

Corollary 7.2.1 (Accuracy Change). Let the change in the confusion matrix of a node C_n^{l-1} , caused due a change of performance of the diagnosis algorithm deployed at the node follows the pattern in Table 7.1 for a state f_k . Let $\theta' = (c_{k,k} - \delta) / ((\sum_{j=0}^{K_n} c_{j,k}) - \delta)$. Then, the accuracy of identifying the state f_k can be expressed in the form $a_{f_k}^{l-1} = a_k\theta' + b_k$; where a_k and b_k are real-valued numbers.

Proof. The proof is only a generalization of the Proposition 7.2.1 that follows along the same lines as in the proof of Proposition 7.2.1 for f_k with a confusion matrix where δ is associated with f_k , and $\rho_k\delta$ is associated with the other health states. It is clear that for a change δ in any mode f_k (instead of the 1-st fault mode f_1) at any component at a given level l , the accuracy $a_{f_k}^l$ can be expressed in the form $a_k\theta' + b_k$; where a_k and b_k are real numbers that are independent of δ and ρ_k . \square

Proposition 7.2.2 (Accuracy Change). Let the change in the confusion matrix of a node C_1^{l-1} , caused due a change of performance of the diagnosis algorithm deployed at the node is according to Table 7.1. Let $\theta = (c_{1,1} - \delta)/((\sum_{j=0}^{K_1} c_{j,1}) - \delta)$. Then, the change in the accuracy of identifying the health state f_k , where $f_k \neq f_1$, is negligible for a sufficiently small δ .

Proof. The proof is similar to that of the Proposition 7.2.1. The key difference between the above two propositions is that here we are interested in the accuracy of f_k compared to f_1 while the change δ is still associated with f_1 . Recall that for computing hierarchical agreement factors in Chapter 6, the accuracy $a_{f_1}^{l-1}$ with which the health state f_1 is identified at level $l - 1$ is computed by constructing a 2×2 dimensional “one-versus-all” decision matrix \mathbf{C}_k (as discussed in Section 6.2.2), where $k \neq 1$. Let \mathbf{C}_{con} denote an $(K_1 + 1) \times (K_1 + 1)$ confusion matrix that is associated with the $K_1 + 1$ health states of the node C_1^{l-1} as shown in Table 7.1. Let $c_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_{con} , and $c'_{i,j}$ denote the element in the i -th row and the j -th column of \mathbf{C}_1 . The elements of the \mathbf{C}_k matrix are changed due to the change in the confusion matrix of a node C_1^{l-1} as follows:

- $c'_{2,2} = c_{k,k}$ remains unchanged despite the change in the confusion matrix,
- $c'_{2,1} = \left(\sum_{j=0}^{K_1} c_{k,j} \right) - c_{k,k} = \kappa_{21}$ remains unchanged despite the change in the confusion matrix,
- $c'_{1,2} = \kappa_{12} + \rho_k \delta$ where $\kappa_{12} = \left(\sum_{j=0}^{K_1} c_{j,k} \right) - c_{k,k}$ is the value of $c'_{1,2}$ when $\delta = 0$ (without any change in the confusion matrix), and
- $c'_{1,1} = \text{sum}(\mathbf{C}_{con}) - c'_{2,2} - c'_{2,1} - c'_{1,1} = \kappa_{11} - \rho_k \delta$ where κ_{11} is the value of $c'_{1,1}$ when $\delta = 0$ (without any change in the confusion matrix).

Note that $\text{sum}(\mathbf{C}_{con})$ remains the same despite the change in the confusion

matrix. The accuracy of identifying the k -st health state is computed as follows:

$$\begin{aligned} a_{f_k}^{l-1} &= \text{trace}(\mathbf{C}_1) / \text{sum}(\mathbf{C}_1) \\ &= \frac{\kappa_{11} + c_{k,k} - \rho_k \delta}{\kappa_{11} + c_{k,k} + \kappa_{12} + \kappa_{21}} \end{aligned}$$

Since $(\kappa_{11} + c_{k,k} + \kappa_{12} + \kappa_{21}) \gg \rho_k \delta$, the accuracy is reduced by a negligible amount $(\rho_k \delta) / (\kappa_{11} + c_{k,k} + \kappa_{12} + \kappa_{21})$. \square

We are now in a position where in the remainder of this section we investigate the four general cases 1 to 4 corresponding to the initial distributions that are stated earlier.

Case 1: *The initial distribution that corresponds to the faulty state f_1 of C_1^{l-1} .*

From Equation (6.3), the probability distribution over X_p^l is computed as follows:

$$\begin{aligned} &P(X_p^l | X_1^{l-1} = f_1, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0) \\ &\approx \left(P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f), P(X_p^l = x_1 | X_1^{l-1} = f_1), \right. \\ &\quad \left. P(X_p^l = x_2 | X_1^{l-1} = f_1), \dots, P(X_p^l = x_N | X_1^{l-1} = f_1) \right) \end{aligned} \quad (7.1)$$

where the first term is conditioned on the health states of all the parent sub-components at level $l - 1$ with $f \neq f_0$ for the 1-st sub-component, and $f = f_0$ otherwise.

From Equation (6.6), the probability $P(X_p^l = x_1 | X_1^{l-1} = f_1)$ is expressed as

follows:

$$\begin{aligned}
P(X_p^l = x_1 | X_1^{l-1} = f_1) &\approx P(X_p^l = x_1 | I_1^{l-1} = f_1) \\
&= h_{1,1}^{p,1} \left(P(X_1^{l-1} = f_1 | I_1^{l-1} = f_1) + \sum_{j=2}^{K_1} P(X_1^{l-1} = f_j | I_1^{l-1} = f_1) \right) \\
&= h_{1,1}^{p,1} \left(\frac{c_{1,1} - \delta}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} + \frac{\sum_{j=2}^{K_1} c_{j,1}}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \right) \\
&= h_{1,1}^{p,1} \left(\theta + \frac{(\sum_{j=0}^{K_1} c_{j,1}) - c_{0,1} - c_{1,1}}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \right) \\
&= h_{1,1}^{p,1} \left(\theta + \frac{\kappa_0}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \right)
\end{aligned} \tag{7.2}$$

where κ_0 is a parameter independent of δ and ρ_k . By the definition of θ , $(\sum_{j=0}^{K_1} c_{j,1}) - \delta$ can be expressed as $(c_{1,1} - \delta)/\theta$. Consequently, $P(X_p^l = x_1 | X_1^{l-1} = f_1)$ above becomes:

$$P(X_p^l = x_1 | X_1^{l-1} = f_1) = h_{1,1}^{p,1} \left(\theta + \frac{\kappa_0 \theta}{c_{1,1} - \delta} \right) = h_{1,1}^{p,1} \theta \left(1 + \frac{\kappa_0}{c_{1,1} - \delta} \right) \tag{7.3}$$

In Equation (7.3), $\kappa_0 = 0$ if none of the f_1 fault cases are misidentified as other faults in the confusion matrix. Usually, $c_{1,1} \gg \kappa_0$ and for small change in δ , $c_{1,1} \gg \delta$. Therefore, the effects of δ are to be considered as negligible in Equation (7.3). Furthermore, since the hierarchical agreement factor $h_{1,1}^{p,1}$ in Equation (7.3) is a ratio of two accuracies (as described in Chapter 6), and the decreased accuracy at level $l - 1$ satisfies Proposition 7.2.1, the probability $P(X_p^l = x_1 | X_1^{l-1} = f_1)$ can be expressed as follows:

$$P(X_p^l = x_1 | X_1^{l-1} = f_1) = a_1 \theta^2 + b_1 \theta + c_1 \tag{7.4}$$

where a_1 , b_1 , and c_1 are real numbers.

Next, from Equation (6.7), the probability $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f)$ is expressed

as follows:

$$\begin{aligned}
& P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) \\
& \approx P(X_p^l = x_0 | I_1^{l-1} = f_1) \prod_{j=2}^N P(X_p^l = x_0 | I_j^{l-1} = f_0) \\
& = (1 - h_{1,1}^{p,1}) P(X_1^{l-1} = f_0 | I_1^{l-1} = f_1) \prod_{j=2}^N h_{j,0}^{p,0} P(X_j^{l-1} = f_0 | I_j^{l-1} = f_0) \\
& = (1 - h_{1,1}^{p,1}) \frac{c_{0,1}}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \prod_{j=2}^N h_{j,0}^{p,0} P(X_j^{l-1} = f_0 | I_j^{l-1} = f_0)
\end{aligned} \tag{7.5}$$

The probabilities inside the product in Equation (7.5) are determined from the unchanged confusion matrices of the other parent nodes of C_p^l , and the product is a real number κ_1 . Hence, Equation (7.5) becomes:

$$P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) = (1 - h_{1,1}^{p,1}) \kappa_1 \frac{c_{0,1}}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \tag{7.6}$$

and the last factor in Equation (7.6) can be expressed as follows:

$$\begin{aligned}
\frac{c_{0,1}}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} &= \left(1 - \frac{c_{0,1}^-}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \right) \\
&= \left(1 - \frac{c_{1,1} - \delta}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} - \frac{c_{2,1}^+, \dots, +c_{K_1,1}}{(\sum_{j=0}^{K_1} c_{j,1}) - \delta} \right) \\
&= 1 - \theta - \kappa_2
\end{aligned} \tag{7.7}$$

where κ_2 is real number that is independent of δ and ρ_k . Therefore, combining Equations (7.6) and (7.7) we get,

$$P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) = (1 - h_{1,1}^{p,1}) \kappa_1 (1 - \theta - \kappa_2) \tag{7.8}$$

As explained above, $h_{1,1}^{p,1}$ has the form in Proposition 7.2.1 and κ_1 is a real number. Consequently, $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f)$ in Equation (7.8) can be expressed

as follows:

$$P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) = a_0\theta^2 + b_0\theta + c_0 \quad (7.9)$$

where a_0 , b_0 , and c_0 are real numbers. Next, from Equation (6.8), the remaining probabilities $P(X_p^l = x_n | X_1^{l-1} = f_1)$, where $n = 2, \dots, N$, are expressed as follows:

$$\begin{aligned} &P(X_p^l = x_n | X_1^{l-1} = f_1) \\ &= \frac{1}{N-1} \left(1 - P(X_p^l = x_1 | X_1^{l-1} = f_1) - P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) \right) \end{aligned} \quad (7.10)$$

From Equations (7.4) and (7.9), the probability $P(X_p^l = x_n | X_1^{l-1} = f_1)$ in Equation (7.10) can be expressed as follows:

$$P(X_p^l = x_n | X_1^{l-1} = f_1) = a_n\theta^2 + b_n\theta + c_n \quad (7.11)$$

where a_n , b_n , and c_n are real numbers.

Remark 7.2.1 (Parameter Variation). From Equations (7.4), (7.9), and (7.11), the probability distribution of Equation (7.1) can be expressed in the form:

$$\begin{aligned} &P(X_p^l | X_1^{l-1} = f_1, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0) \\ &= \left((a_0\theta^2 + b_0\theta + c_0), (a_1\theta^2 + b_1\theta + c_1), \dots, (a_N\theta^2 + b_N\theta + c_N) \right) \end{aligned}$$

Case 2: *The initial distribution that corresponds to the other faulty state f_k of C_1^{l-1} , where $k = 2, \dots, K_1$.*

From Equation (6.3), the probability distribution over X_p^l is computed as

follows:

$$\begin{aligned}
& P(X_p^l | X_1^{l-1} = f_k, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0) \\
& \approx \left(P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f), P(X_p^l = x_1 | X_1^{l-1} = f_k), \right. \\
& \quad \left. P(X_p^l = x_2 | X_1^{l-1} = f_k), \dots, P(X_p^l = x_N | X_1^{l-1} = f_k) \right)
\end{aligned} \tag{7.12}$$

where the first term is conditioned on the health states of all the parent sub-components at level $l - 1$ with $f \neq f_0$ for the 1-st sub-component, and $f = f_0$ otherwise.

From Equation (6.6), the probability $P(X_p^l = x_1 | X_1^{l-1} = f_k)$ is expressed as follows:

$$\begin{aligned}
P(X_p^l = x_1 | X_1^{l-1} = f_k) & \approx P(X_p^l = x_1 | I_1^{l-1} = f_k) \\
& = h_{1,k}^{p,1} \left(P(X_1^{l-1} = f_k | I_1^{l-1} = f_k) + \sum_{j \neq k, j=2}^{K_1} P(X_1^{l-1} = f_j | I_1^{l-1} = f_k) \right) \\
& = h_{1,k}^{p,1} \left(\frac{c_{k,k}}{(\sum_{j=0}^{K_1} c_{j,k}) + \rho_k \delta} + \frac{(c_{1,k} + \rho_k \delta) + \sum_{j \neq k, j=2}^{K_1} c_{j,k}}{(\sum_{j=0}^{K_1} c_{j,k}) + \rho_k \delta} \right) \\
& = h_{1,k}^{p,1} \left(\frac{(\sum_{j=1}^{K_1} c_{j,k}) + \rho_k \delta}{(\sum_{j=0}^{K_1} c_{j,k}) + \rho_k \delta} \right) \\
& = h_{1,k}^{p,1} \left(\frac{(\sum_{j=0}^{K_1} c_{j,k}) - c_{0,k} + \rho_k \delta}{(\sum_{j=0}^{K_1} c_{j,k}) + \rho_k \delta} \right)
\end{aligned} \tag{7.13}$$

It is easy to see that $\sum_{j=0}^{K_1} c_{j,k} \gg \rho_k \delta$, as δ represents a small change and $\rho_k \delta$ is a fraction of δ . Therefore, the effects of the change in the confusion matrix at node C_1^{l-1} is negligible on the second factor in Equation (7.13). By Proposition 7.2.2, the factor $h_{1,k}^{p,1}$ in Equation (7.13) is considered to be negligibly affected by the change in δ as well.

From Equation (6.7), the probability $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f)$ is expressed as

follows:

$$\begin{aligned}
& P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) \\
& \approx P(X_p^l = x_0 | I_1^{l-1} = f_k) \prod_{j=2}^N P(X_p^l = x_0 | I_j^{l-1} = f_0) \\
& = (1 - h_{1,k}^{p,1}) P(X_1^{l-1} = f_0 | I_1^{l-1} = f_k) \prod_{j=2}^N h_{j,0}^{p,0} P(X_j^{l-1} = f_0 | I_j^{l-1} = f_0)
\end{aligned} \tag{7.14}$$

The last term that consists of the product in Equation (7.14) is computed from the unchanged confusion matrices of the other parent nodes of C_p^l , and the product is a real number that is unaffected by the change in the confusion matrix at node C_1^{l-1} . As found above, $h_{1,k}^{p,1}$ is considered to be negligibly affected by the change in the confusion matrix. Consequently, the term $(1 - h_{1,k}^{p,1})$ is considered to be negligibly affected by the change in the confusion matrix at node C_1^{l-1} . Now,

$$P(X_1^{l-1} = f_0 | I_1^{l-1} = f_k) = \frac{c_{0,k}}{(\sum_{j=0}^{K_1} c_{j,k}) + \rho_k \delta}$$

As found in the analysis of $P(X_p^l = x_1 | X_1^{l-1} = f_k)$ above, $\sum_{j=0}^{K_1} c_{j,k} \gg \rho_k \delta$, and consequently, the probability $P(X_1^{l-1} = f_0 | I_1^{l-1} = f_k)$ is considered to be negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

From Equation (6.8), the remaining probabilities $P(X_p^l = x_n | X_1^{l-1} = f_k)$, where $n = 2, \dots, N$, are expressed as follows:

$$\begin{aligned}
& P(X_p^l = x_n | X_1^{l-1} = f_k) \\
& = \frac{1}{N-1} \left(1 - P(X_p^l = x_1 | X_1^{l-1} = f_k) - P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) \right)
\end{aligned} \tag{7.15}$$

From the analysis of the probabilities $P(X_p^l = x_1 | X_1^{l-1} = f_k)$ and $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f)$ above, it follows that the probability $P(X_p^l = x_n | X_1^{l-1} = f_k)$ in Equation (7.15) is negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

Remark 7.2.2 (Parameter Variation). From the analysis of the probabilities $P(X_p^l = x_1|X_1^{l-1} = f_k)$, $P(X_p^l = x_0|X_{1,\dots,N}^{l-1} = f)$ and $P(X_p^l = x_n|X_1^{l-1} = f_k)$ above, it follows that the probability distribution in Equation (7.12) is negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

Case 3: *The initial distributions that correspond to the faults in the other parent nodes of C_p^l .*

From Equation (6.3), the probability distribution over X_p^l is computed as follows:

$$\begin{aligned} & P(X_p^l|X_1^{l-1} = f_0, \dots, X_n^{l-1} = f_k, \dots, X_N^{l-1} = f_0) \\ & \approx \left(P(X_p^l = x_0|X_{1,\dots,N}^{l-1} = f), P(X_p^l = x_1|X_n^{l-1} = f_k), \right. \\ & \quad \left. \dots P(X_p^l = x_n|X_n^{l-1} = f_k), \dots, P(X_p^l = x_N|X_n^{l-1} = f_k) \right) \end{aligned} \quad (7.16)$$

where $n = 2, \dots, N$; $k = 1, \dots, K_n$; and the first term is conditioned on the health states of all the parent sub-components at level $l - 1$ with $f \neq f_0$ for the n -th sub-component that is faulty, and $f = f_0$ otherwise.

From Equation (6.6), the probability $P(X_p^l = x_n|X_n^{l-1} = f_k)$ is expressed as follows:

$$\begin{aligned} & P(X_p^l = x_n|X_n^{l-1} = f_k) \approx P(X_p^l = x_n|I_n^{l-1} = f_k) \\ & = h_{n,k}^{p,n} \left(P(X_n^{l-1} = f_k|I_n^{l-1} = f_k) + \sum_{j \neq k, j=1}^{K_n} P(X_n^{l-1} = f_j|I_n^{l-1} = f_k) \right) \end{aligned} \quad (7.17)$$

All the probabilities on the right-hand side of Equation (7.17) correspond to the parent nodes of C_p^l whose confusion matrices remain unchanged. Therefore, the probability $P(X_p^l = x_n|X_n^{l-1} = f_k)$ is unaffected by the change in the confusion matrix at node C_1^{l-1} .

From Equation (6.7), the probability $P(X_p^l = x_0|X_{1,\dots,N}^{l-1} = f)$ is expressed as

follows:

$$\begin{aligned}
& P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) \\
& \approx P(X_p^l = x_0 | I_n^{l-1} = f_k) \prod_{j \neq n, j=1}^N P(X_p^l = x_0 | I_j^{l-1} = f_0) \\
& = (1 - h_{n,k}^{p,n}) P(X_n^{l-1} = f_0 | I_n^{l-1} = f_k) \prod_{j \neq n, j=1}^N h_{j,0}^{p,0} P(X_j^{l-1} = f_0 | I_j^{l-1} = f_0)
\end{aligned} \tag{7.18}$$

Equation (7.18) can be rearranged as:

$$\begin{aligned}
P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) &= (1 - h_{n,k}^{p,n}) P(X_n^{l-1} = f_0 | I_n^{l-1} = f_k) \\
& h_{1,0}^{p,0} P(X_1^{l-1} = f_0 | I_1^{l-1} = f_0) \prod_{j \neq n, j=2}^N h_{j,0}^{p,0} P(X_j^{l-1} = f_0 | I_j^{l-1} = f_0)
\end{aligned} \tag{7.19}$$

In Equation (7.19), all the factors, except $h_{1,0}^{p,0}$ and $P(X_1^{l-1} = f_0 | I_1^{l-1} = f_0)$, correspond to the parent nodes of C_p^l whose confusion matrices remain unchanged, and are unaffected by the change in the confusion matrix at node C_1^{l-1} . By Proposition 7.2.2, there are negligible effects of the change in the confusion matrix at node C_1^{l-1} on $h_{1,0}^{p,0}$. Furthermore,

$$P(X_1^{l-1} = f_0 | I_1^{l-1} = f_0) = \frac{c_{0,0}}{\left(\sum_{j=0}^{K_1} c_{j,0} \right) + \rho_0 \delta}$$

In general, $\sum_{j=0}^{K_1} c_{j,0} \gg \rho_0 \delta$. Therefore, there is a negligible effect of the change in the confusion matrix at node C_1^{l-1} on $P(X_1^{l-1} = f_0 | I_1^{l-1} = f_0)$.

From Equation (6.8), the remaining probabilities $P(X_p^l = x_{n'} | X_1^{l-1} = f_k)$, where n' represents all the healthy subcomponent of C_p^l except C_n^{l-1} , are expressed as follows:

$$\begin{aligned}
& P(X_p^l = x_{n'} | X_1^{l-1} = f_k) \\
& = \frac{1}{N-1} \left(1 - P(X_p^l = x_n | X_n^{l-1} = f_k) - P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f) \right)
\end{aligned} \tag{7.20}$$

From the analysis of the probabilities $P(X_p^l = x_n | X_n^{l-1} = f_k)$ and $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f)$ above, it follows that the probability $P(X_p^l = x_{n'} | X_1^{l-1} = f_k)$ in Equation (7.20) is negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

Remark 7.2.3 (Parameter Variation). By the analysis of the probabilities $P(X_p^l = x_n | X_n^{l-1} = f_k)$, $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f)$ and $P(X_p^l = x_{n'} | X_1^{l-1} = f_k)$ above, it follows that the probability distribution in Equation (7.16) is negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

Case 4: *The initial distribution that corresponds to the situation when all parent nodes of C_p^l are healthy.*

From Equation (6.3), the probability distribution over X_p^l is computed as follows:

$$\begin{aligned} & P(X_p^l | X_1^{l-1} = f_0, X_2^{l-1} = f_0, \dots, X_N^{l-1} = f_0) \\ & \approx \left(P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0), P(X_p^l = x_1 | X_{1,\dots,N}^{l-1} = f_0), \right. \\ & \quad \left. P(X_p^l = x_2 | X_{1,\dots,N}^{l-1} = f_0), \dots, P(X_p^l = x_N | X_{1,\dots,N}^{l-1} = f_0) \right) \end{aligned} \quad (7.21)$$

where each term is conditioned on the healthy states of all the parent sub-components at level $l - 1$.

From Equation (6.9), the probability $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0)$ is expressed as follows:

$$\begin{aligned} & P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0) \\ & = 1 - P(X_p^l = \bar{x}_0 | X_{1,\dots,N}^{l-1} = f_0) \\ & = 1 - \prod_{j=1}^N (1 - h_{j,0}^{p,0}) P(X_j^{l-1} = \bar{f}_0 | I_j^{l-1} = f_0) \end{aligned} \quad (7.22)$$

where \bar{x}_0 and \bar{f}_0 correspond to the set $\{X_p^l\} \setminus x_0$ and $\{X_n^{l-1}\} \setminus f_0$, respectively depending on the level in the hierarchy. Equation (7.22) can be re-written as:

$$\begin{aligned}
& P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0) \\
&= 1 - \left((1 - h_{1,0}^{p,0}) P(X_1^{l-1} = \bar{f}_0 | I_1^{l-1} = f_0) \right. \\
&\quad \left. \prod_{j=2}^N (1 - h_{j,0}^{p,0}) P(X_j^{l-1} = \bar{f}_0 | I_j^{l-1} = f_0) \right)
\end{aligned} \tag{7.23}$$

In equation (7.23), all the factors, except $(1 - h_{1,0}^{p,0})$ and $P(X_1^{l-1} = \bar{x}_0 | I_1^{l-1} = f_0)$, correspond to the parent nodes of C_p^l whose confusion matrices remain unchanged, and are unaffected by the change in the confusion matrix at node C_1^{l-1} . From Proposition 7.2.2, there are negligible effects of the change in the confusion matrix at node C_1^{l-1} on $h_{1,0}^{p,0}$. Furthermore,

$$P(X_1^{l-1} = \bar{f}_0 | I_1^{l-1} = f_0) = \frac{\sum_{j=1}^{K_1} c_{j,0}}{\left(\sum_{j=0}^{K_1} c_{j,0} \right) + \rho_0 \delta}$$

Since $\sum_{j=0}^{K_1} c_{j,0} \gg \rho_0 \delta$, there is a negligible effect of the change in the confusion matrix at node C_1^{l-1} on $P(X_1^{l-1} = \bar{f}_0 | I_1^{l-1} = f_0)$.

From Equation (6.10), the remaining probabilities $P(X_p^l = x_n | X_{1,\dots,N}^{l-1} = f_0)$, where $n = 1, \dots, N$, are expressed as follows:

$$P(X_p^l = x_n | X_{1,\dots,N}^{l-1} = f_0) = \frac{1}{N} \left(1 - P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0) \right) \tag{7.24}$$

From the analysis of the probability $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0)$ above, it follows that the probability $P(X_p^l = x_n | X_{1,\dots,N}^{l-1} = f_0)$ in equation (7.24) is negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

Remark 7.2.4 (Parameter Variation). From the analysis of the probabilities $P(X_p^l = x_0 | X_{1,\dots,N}^{l-1} = f_0)$ and $P(X_p^l = x_n | X_{1,\dots,N}^{l-1} = f_0)$ above, it follows that the

probability distribution in Equation (7.21) is negligibly affected by the change in the confusion matrix at node C_1^{l-1} .

The following results utilize the notion of a probability potential ϕ that was reviewed in Section 2.2.1.

Lemma 7.2.1 (Parameter Variation). Let $\phi(V)$ denote a potential over the variables \mathcal{V} . Let $X \in V$, and let \mathbf{v}^* be a set of configurations over $V \setminus \{X\}$. Let all entries in $\phi(V)$ be real numbers except for $\phi(X, \mathbf{v}^*)$ which is in the form $(\alpha_0\theta^2 + \beta_0\theta + \gamma_0, \dots, \alpha_N\theta^2 + \beta_N\theta + \gamma_N)$. Then

$$\sum_V \phi(V) = \alpha\theta^2 + \beta\theta + \gamma$$

where α , β , and γ are real numbers.

Proof. Let V^* be the set of all configurations in $\text{span}(\mathcal{V})$ except for the (X, \mathbf{v}^*) -configurations. Then

$$\sum_V \phi(V) = \sum_{V^*} \phi(V) + \sum_X \phi(X, \mathbf{v}^*)$$

The first term is equivalent to a real number γ^* , and the second term is the sum of the $(\alpha_0\theta^2 + \beta_0\theta + \gamma_0) \dots (\alpha_N\theta^2 + \beta_N\theta + \gamma_N)$ entries for all (X, \mathbf{v}^*) -configurations. Hence,

$$\begin{aligned} \sum_V \phi(V) &= \left(\sum_i \alpha_i \right) \theta^2 + \left(\sum_i \beta_i \right) \theta + \left(\sum_i \gamma_i \right) + \gamma^* \\ &= \alpha\theta^2 + \beta\theta + \gamma \end{aligned}$$

where α , β , and γ are real numbers. □

Theorem 7.2.1 ($P(e)$ as a function of a parameter). Let the CDM be a Bayesian network over the universe \mathcal{U} . Let θ be a parameter and let e denote

the evidence that is entered in the CDM. Then assuming that some distributions are in the form $(\alpha_0\theta^2 + \beta_0\theta + \gamma_0, \dots, \alpha_N\theta^2 + \beta_N\theta + \gamma_N)$, we have

$$P(e)(\theta) = \alpha\theta^2 + \beta\theta + \gamma$$

where α , β , and γ are real numbers.

Proof. The proof is similar to that of Theorem 2.2.1 in Chapter 2. Let $U = \{X\} \cup \{X_1, \dots, X_n\}$, $fa(X) = \{X\} \cup pa(X)$ and let π denote a set of parent configurations for which $P(X|\pi_i) = (\alpha_0\theta^2 + \beta_0\theta + \gamma_0, \dots, \alpha_N\theta^2 + \beta_N\theta + \gamma_N)$. Let the evidence potentials be denoted by $\mathbf{e}_1, \dots, \mathbf{e}_m$. Now

$$\begin{aligned} P(e) &= \sum_U P(U, e) = \sum_U P(X|pa(X)) \prod_i P(X_i|pa(X_i)) \prod_j \mathbf{e}_j \\ &= \sum_{fa(X)} P(X|pa(X)) \sum_{U \setminus fa(X)} \prod_i P(X_i|pa(X_i)) \prod_j \mathbf{e}_j \end{aligned}$$

The factor $\sum_{U \setminus fa(X)} \prod_i P(X_i|pa(X_i)) \prod_j \mathbf{e}_j$ is a potential, denoted by $\phi(fa(X))$, with only real numbers, and we have

$$P(e) = \sum_{fa(X)} P(X|pa(X)) \phi(fa(X))$$

The product $P(X|pa(X))\phi(fa(X))$ is a potential satisfying the conditions in Lemma 7.2.1, and we can conclude that

$$P(e)(\theta) = \alpha\theta^2 + \beta\theta + \gamma$$

where α , β , and γ are real numbers. □

Corollary 7.2.2 ($P(X|e)$ as a function of a parameter). Let the CDM be a Bayesian network over the universe \mathcal{U} . Let θ be a parameter and let e denote the evidence that is entered in the CDM, and let \mathbf{u}^* be a set of configurations over

$U \setminus \{X\}$. Let x_i be a state of $X \in \mathcal{U}$. Then assuming a set of $\phi(X, \mathbf{u}^*)$ -configurations in the form $(\alpha_0\theta^2 + \beta_0\theta + \gamma_0, \dots, \alpha_N\theta^2 + \beta_N\theta + \gamma_N)$, $P(X = x_i|e)$ has the form:

$$P(X = x_i|e) = \frac{\alpha\theta^2 + \beta\theta + \gamma}{a\theta^2 + a\theta + c}$$

where $\alpha, \beta, \gamma, a, b$, and c are real numbers.

Proof. The proof follows along the similar lines as in the Theorem 7.2.1, and then follows from the fundamental rule for variables $P(X = x_i|e) = \frac{P(X=x_i,e)}{P(e)}$. \square

7.2.2 Proposed Verification Steps

It is obvious from Remarks 7.2.1 to 7.2.4 of the initial distributions that due to the change in the confusion matrix at node C_1^{l-1} the entries of the CPT that is stored at node C_p^l are either in the form $a\theta^2 + b\theta + c$, or are real numbers that are negligibly changed. This is due to the fact that since the remaining distributions in the CPT are computed by using a weighted-sum of the initial distributions (from Equation (6.12)), the entries corresponding to those distributions are also either in the form $a\theta^2 + b\theta + c$, or are real numbers that are negligibly changed. Given the above observations and Corollary 7.2.2, one can validate a CDM via a sensitivity analysis procedure which allows one to evaluate the behavior of the output(s) of the CDM when a CDM parameter θ (as defined in Section 7.2.1) changes. The sensitivity analysis is a standard procedure for verifying Bayesian networks, and by utilizing Corollary 7.2.2, the procedure becomes straight-forward as described below:

- Step 1. Choose 3 values of δ , namely δ_0, δ_1 , and δ_2 such that the chosen range of δ would cause a small variation in θ in Step 2. The term “small variation” is somewhat subjective and as an example, one may quantify the term by assuming that approximately 0.05 change in the probability θ over the chosen range of δ is a small variation. As an alternative, the variation can also be

quantified easily in terms of the change in the identification accuracy of the fault that is associated with δ .

Step 2. Find the values of θ (as defined in Section 7.2.1), namely θ_0 , θ_1 , and θ_2 that correspond to the three chosen values of δ (here ρ_k values are assumed to be the same, however, one may choose to select different values).

Step 3. For the obtained θ_0 value,

- Compute initial distributions.
- Compute the CPT by using the initial distributions.
- Compute $P(e)(\theta_0)$.
- Introduce and propagate the evidence e under consideration to the network (with the computed CPT) to obtain $P(X = x_1, e)(\theta_0)$

Step 4. Repeat step 3 for θ_1 and θ_2 .

Step 5. Form the following two sets of equations to solve for α , β , γ , a , b , and c :

To determine the coefficients α , β , and γ solve the following:

$$\alpha\theta_0^2 + \beta\theta_0 + \gamma = P(X = x_i, e)(\theta_0)$$

$$\alpha\theta_1^2 + \beta\theta_1 + \gamma = P(X = x_i, e)(\theta_1)$$

$$\alpha\theta_2^2 + \beta\theta_2 + \gamma = P(X = x_i, e)(\theta_2)$$

To determine the coefficients a , b , and c solve the following:

$$a\theta_0^2 + b\theta_0 + c = P(e)(\theta_0)$$

$$a\theta_1^2 + b\theta_1 + c = P(e)(\theta_1)$$

$$a\theta_2^2 + b\theta_2 + c = P(e)(\theta_2)$$

Step 6. Plot $P(X = x_i|e)$ as a function of θ by using the relationship:

$$P(X = x_i|e) = \frac{\alpha\theta^2 + \beta\theta + \gamma}{a\theta^2 + a\theta + c}$$

Determination of Sensitivity: The plot is interpreted as follows. As discussed in Section 7.2, our objective is to perform the verification that the CDM satisfies a more specific requirement, namely that “the model shall be negligibly sensitive to small changes in its parameters”. The term “negligibly” is however somewhat subjective here which can be quantified in terms of the changes in probability values. For any two plotted (refer to Step 6 above) conditional probabilities $P(X = x_1|e)$ and $P(X = x_2|e)$, where $P(X = x_1|e) > P(X = x_2|e)$ (without any variation in model parameters), we consider the model to be negligibly sensitive if the same inequality $P(X = x_1|e) > P(X = x_2|e)$ remains true over the entire range of θ under consideration.

It is important to note that in the above steps, while computing the CPTs by using the computed initial distributions, the weights in the weighted-sum (refer to Equation (6.12)) are kept unchanged. The underlying assumption is that any small change in the sensitivity parameters δ should not affect the way the initial distributions are combined to compute the remaining distributions in the CPT.

7.3 CDM Verification Results

In this section, a number of sample CDM verification results are provided which demonstrate that the sensitivity of the implemented CDM to parameter changes with different fault evidences is negligible. Table 7.2 shows the confusion matrix that corresponds to the node Sat-3 Y-axis RW (C_8^1) of the CDM shown in Figure 6.3 of Chapter 6. Table 7.2 is obtained from Table 5.1 (Chapter 5) by removing the “Ambiguity” column. Here, we consider that there is a change in the performance of

Table 7.2: Confusion Matrix at Sat-3 RW-Y (C_8^1)

Identified → Actual ↓	Healthy	Friction Fault	Current Fault
Healthy	169	3	0
Friction Fault	$11 + \rho_0\delta$	$29 - \delta$	$0 + \rho_2\delta$
Current Fault	2	13	25

the diagnosis algorithm at node C_8^1 , and consequently, in δ cases, the “friction fault” is mis-identified as either the “healthy” case or the “current fault” case. Note that for a given δ , there are various ways in which ρ_k s may be varied. In this investigation we assume that all the ρ_k s are the same, i.e., the number changed/misidentified cases (δ) are distributed evenly among the other health states. Therefore, $\rho_0 = 0.5$ and $\rho_2 = 0.5$. Note that there are infinite possible ways to distribute the number δ mis-identified fault into other health states, and an exhaustive investigation of all such cases is beyond the scope of this thesis.

The results that are presented in the remainder of this section have been obtained by using the Symbolic Math Toolbox in MATLAB (for solving the two sets of equations for sensitivity analysis and for computing the CPTs), and the open source BN tool that is available from [155] (for belief propagation and updating). Note that the same BN tool was utilized for implementing the CDM in Chapter 6). Three possible values of δ are chosen: $\delta_0 = 0$, $\delta_1 = 3$, and $\delta_2 = 6$. The three values of δ were selected such that the chosen range of δ would cause a small variation of approximately 0.05 in θ . Recall that the parameter of our interest is defined as $\theta = (c_{1,1} - \delta) / ((\sum_{j=0}^{K_1} c_{j,1}) - \delta) = (29 - \delta) / (45 - \delta)$. Therefore, for the three chosen values $\delta_0 = 0$, $\delta_1 = 3$ and $\delta_2 = 6$, corresponding values of θ are obtained as $\theta_0 = 0.6444$, $\theta_1 = 0.6190$, and $\theta_2 = 0.5897$, respectively. Table 7.3 quantifies the parameter variations under consideration in terms of the accuracy changes. Note that the approximately 0.05 variation in θ corresponds to approximately 2.4% decrease in the accuracy in identifying the friction fault.

Table 7.3: Fault Identification Accuracy Changes at Sat-3 RW-Y (C_8^1)

Accuracy \rightarrow $\delta \downarrow$	Healthy	Friction Fault	Current Fault
δ_0	93.65%	89.29%	94.05%
δ_1	93.06%	88.10%	93.45%
δ_2	92.46%	86.90%	92.86%

First, let us investigate the outputs/the probabilities $P(X = x_i|e)$, where x_i is a state of Sat-3 ACS in the implemented CDM (refer to Figure 6.3). Let e denote the evidence of the friction fault in Sat-3 Y-axis reaction wheel (RW). Recall from Chapter 6 that the possible states of the ACS are $\{Healthy, RW_X fault, RW_Y fault, RW_Z fault\}$, which are denoted here by x_0, x_1, x_2 and x_3 , respectively. Furthermore, recall that the three possible states of a RW are $\{Healthy, friction fault, current fault\}$, which are denoted here by f_0, f_1 , and f_2 , respectively.

The following results are obtained by executing the Steps 1 to 4 of the verification procedure that is presented in Section 7.2.2.

For $\theta_0 = 0.6444$ we obtain:

The initial distributions:

$$P(ACS|RW_y = f_1) = (0.0034, 0.0597, 0.8772, 0.0597)$$

$$P(ACS|RW_y = f_2) = (0.0000, 0.0050, 0.9900, 0.0050)$$

$$P(ACS|RW_x = f_1) = (0.0034, 0.8772, 0.0597, 0.0597)$$

$$P(ACS|RW_x = f_2) = (0.0000, 0.9900, 0.0050, 0.0050)$$

$$P(ACS|RW_z = f_1) = (0.0034, 0.0597, 0.0597, 0.8772)$$

$$P(ACS|RW_z = f_2) = (0.0000, 0.0050, 0.0050, 0.9900)$$

$$P(ACS|RW_x = f_0, RW_y = f_0, RW_z = f_0) = (0.9970, 0.0010, 0.0010, 0.0010)$$

After recomputing the entire CPT that is stored at Sat-3 ACS node, and propagating the evidence with probability $P(e)(\theta_0) = 0.05$, the following results are obtained (note that the $P(X = x_i, e)(\theta_j)$ values have been normalized to obtain the

sum of the probabilities over the health states x_i equal to 1):

$$P(ACS = x_0, e)(\theta_0) = 0.0042$$

$$P(ACS = x_1, e)(\theta_0) = 0.1003$$

$$P(ACS = x_2, e)(\theta_0) = 0.7952$$

$$P(ACS = x_3, e)(\theta_0) = 0.1003$$

For $\theta_1 = 0.6190$ we obtain:

The initial distributions:

$$P(ACS|RW_y = f_1) = (0.0044, 0.0673, 0.8611, 0.0673)$$

$$P(ACS|RW_y = f_2) = (0.0000, 0.0081, 0.9837, 0.0081)$$

$$P(ACS|RW_x = f_1) = (0.0034, 0.8772, 0.0597, 0.0597)$$

$$P(ACS|RW_x = f_2) = (0.0000, 0.9900, 0.0050, 0.0050)$$

$$P(ACS|RW_z = f_1) = (0.0034, 0.0597, 0.0597, 0.8772)$$

$$P(ACS|RW_z = f_2) = (0.0000, 0.0050, 0.0050, 0.9900)$$

$$P(ACS|RW_x = f_0, RW_y = f_0, RW_z = f_0) = (0.9964, 0.0012, 0.0012, 0.0012)$$

After recomputing the entire CPT that is stored at Sat-3 ACS node, and propagating the evidence with probability $P(e)(\theta_1) = 0.05$, the following results are obtained (note that the $P(X = x_i, e)(\theta_j)$ values have been normalized to obtain the sum of the probabilities over the health states x_i equal to 1):

$$P(ACS = x_0, e)(\theta_1) = 0.0051$$

$$P(ACS = x_1, e)(\theta_1) = 0.1071$$

$$P(ACS = x_2, e)(\theta_1) = 0.7807$$

$$P(ACS = x_3, e)(\theta_1) = 0.1071$$

For $\theta_2 = 0.5897$ we obtain:

The initial distributions:

$$P(ACS|RW_y = f_1) = (0.0055, 0.0750, 0.8444, 0.0750)$$

$$P(ACS|RW_y = f_2) = (0.0000, 0.0113, 0.9774, 0.0113)$$

$$P(ACS|RW_x = f_1) = (0.0032, 0.8772, 0.0598, 0.0598)$$

$$P(ACS|RW_x = f_2) = (0.0000, 0.9900, 0.0050, 0.0050)$$

$$P(ACS|RW_z = f_1) = (0.0032, 0.0598, 0.0598, 0.8772)$$

$$P(ACS|RW_z = f_2) = (0.0000, 0.0050, 0.0050, 0.9900)$$

$$P(ACS|RW_x = f_0, RW_y = f_0, RW_z = f_0) = (0.9957, 0.0014, 0.0014, 0.0014)$$

After recomputing the entire CPT that is stored at Sat-3 ACS node, and propagating the evidence with probability $P(e)(\theta_2) = 0.05$, the following results are obtained (note that the $P(X = x_i, e)(\theta_j)$ values have been normalized to obtain the sum of the probabilities over the health states x_i equal to 1):

$$P(ACS = x_0, e)(\theta_2) = 0.0061$$

$$P(ACS = x_1, e)(\theta_2) = 0.1141$$

$$P(ACS = x_2, e)(\theta_2) = 0.7656$$

$$P(ACS = x_3, e)(\theta_2) = 0.1142$$

Note that $pa(C_8^1) = \emptyset$, and $P(e)$ are the same in all cases. It is also worthwhile to note that the initial distribution $P(ACS|RW_y = f_1)$ above corresponds to the analysis in the Case 1 in Section 7.2.1, $P(ACS|RW_y = f_2)$ above corresponds to the analysis in the Case 2 in Section 7.2.1, and $P(ACS|RW_x = f_0, RW_y = f_0, RW_z = f_0)$ above corresponds to the analysis in the Case 4 in Section 7.2.1. The remaining four initial distributions correspond to the analysis in the Case 3 in Section 7.2.1.

It is easily verifiable that the approximations that are made in the analysis in Section 7.2.1 are justified with an exception of the initial distribution $P(ACS|RW_y = f_2)$. It is observed that with the variation of the parameter θ , the changes in this distribution is noticeable. This is due to the fact that in the confusion matrix shown in Table 7.2, the approximation $\sum_{j=0}^{K_1} c_{j,k} \gg \rho_k \delta$ is not valid. This is due to the fact that an unusually high number of the “current fault” cases were mis-identified as the “friction fault” which caused the sum to become unexpectedly low. However,

it is important to note that although the change in $P(ACS|RW_y = f_2)$ is noticeable, it is less than that in $P(ACS|RW_y = f_1)$ which varies as $a_n\theta^2 + b_n\theta + c_n$ (the degree of the polynomial is of at the most 2) where a_n , b_n , and c_n are real numbers. Consequently, Lemma 7.2.1, Theorem 7.2.1, and Corollary 7.2.2 are still valid for the obtained results.

Figure 7.2 shows the outputs under consideration that are obtained from the Step 6 of the verification procedure (after determining the polynomial coefficients in Step 5 of the procedure). It is observed that for small variations in the network

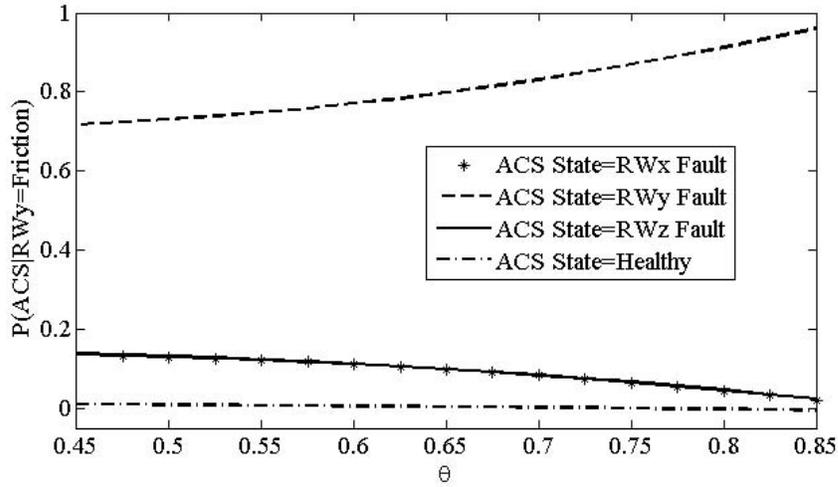


Figure 7.2: Sensitivity of Sat-3 ACS states (subsystem level) given a friction fault evidence at Sat-3 RW_y (component level).

parameters, there is a negligible change in the state of the ACS which implies that when there is an evidence of a friction fault in the Y axis RW (component level), the probability that the Y axis RW is faulty remains the highest (in the subsystem level) despite the parameter variations. This indicates that the CDM is not too sensitive to small variations in the network parameters, as desired.

Next, Figure 7.3 shows the same outputs with the evidence e as the current fault in Sat-3 X -axis RW. This again indicates that the CDM is not sensitive to small variations in the network parameters, as desired. Note that Figure 7.3 was

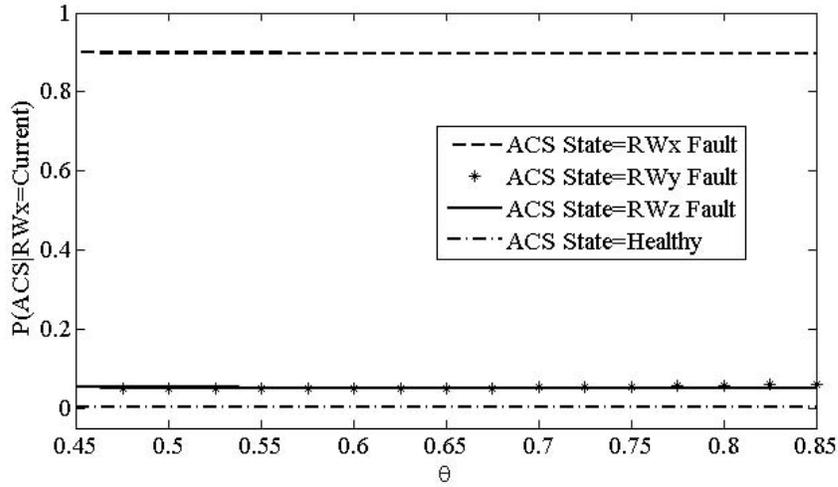


Figure 7.3: Sensitivity of Sat-3 ACS states (subsystem level) given a current fault evidence at Sat-3 RW_x (component level).

generated by using the following information that are obtained with the recomputed CPT that is stored at the Sat-3 ACS node, and finally propagating the evidence with the probability $P(e)(\theta_2) = 0.05$, namely (as before, the $P(X = x_i, e)(\theta_j)$ values have been normalized to obtain the sum of the probabilities over the health states x_i equal to 1):

For $\theta_0 = 0.6444$ we obtain:

$$P(ACS = x_0, e)(\theta_0) = 0.0012$$

$$P(ACS = x_1, e)(\theta_0) = 0.8971$$

$$P(ACS = x_2, e)(\theta_0) = 0.0509$$

$$P(ACS = x_3, e)(\theta_0) = 0.0509$$

For $\theta_1 = 0.6190$ we obtain:

$$P(ACS = x_0, e)(\theta_1) = 0.0012$$

$$P(ACS = x_1, e)(\theta_1) = 0.8973$$

$$P(ACS = x_2, e)(\theta_1) = 0.0503$$

$$P(ACS = x_3, e)(\theta_1) = 0.0511$$

For $\theta_2 = 0.5897$ we obtain:

$$P(ACS = x_0, e)(\theta_1) = 0.0012$$

$$P(ACS = x_1, e)(\theta_1) = 0.8976$$

$$P(ACS = x_2, e)(\theta_1) = 0.0498$$

$$P(ACS = x_3, e)(\theta_1) = 0.0514$$

Finally, let us investigate the outputs $P(X = x_i|e)$, where x_i is a state of Sat-3 Y-axis RW in the implemented CDM (refer to Figure 6.3). Let e denote the evidence $RW_Y fault$ in Sat-3 ACS. With the given three selected values $\theta_1 = 0.6444$, $\theta_2 = 0.6190$, and $\theta_3 = 0.5897$, the following results are obtained (note that the computed initial distributions are the same as above, and we are considering here a different evidence and a different hypothesis variable):

For $\theta_0 = 0.6444$ we have:

$$P(e) = 0.0909$$

$$P(RW_y = f_0, e)(\theta_0) = 0.0689$$

$$P(RW_y = f_1, e)(\theta_0) = 0.4375$$

$$P(RW_y = f_2, e)(\theta_0) = 0.4936$$

For $\theta_1 = 0.6190$ we have:

$$P(e) = 0.0900$$

$$P(RW_y = f_0, e)(\theta_1) = 0.0712$$

$$P(RW_y = f_1, e)(\theta_1) = 0.4336$$

$$P(RW_y = f_2, e)(\theta_1) = 0.4952$$

For $\theta_2 = 0.5897$:

$$P(e) = 0.0891$$

$$P(RW_y = f_0, e)(\theta_2) = 0.0736$$

$$P(RW_y = f_1, e)(\theta_2) = 0.4295$$

$$P(RW_y = f_2, e)(\theta_2) = 0.4969$$

As in the above earlier cases, the $P(X = x_i, e)(\theta_j)$ values have been normalized to obtain the sum of the probabilities over the health states x_i equal to 1. Figure 7.4 shows the output under consideration that is obtained from step 6 of the validation procedure (after determining the polynomial coefficients in step 5 of the procedure). It is observed that as before, for the small variations in the network parameters,

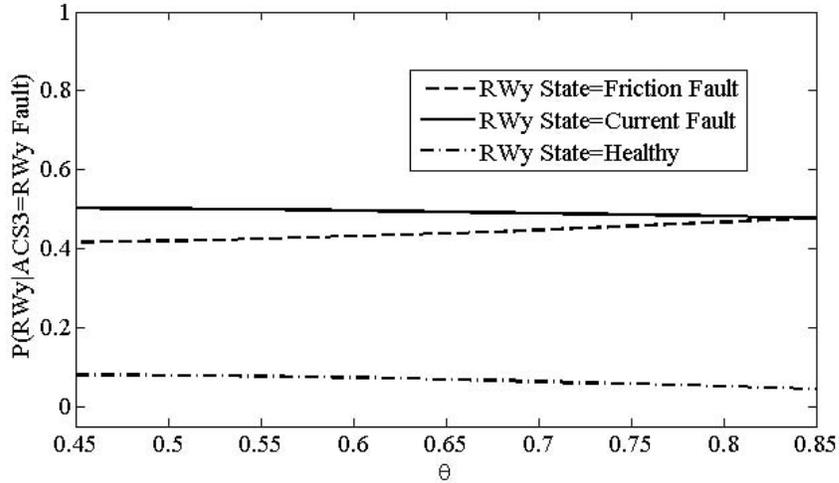


Figure 7.4: Sensitivity of Sat-3 RW_y states (component level) given a fault evidence at Sat-3 ACS (subsystem level).

there is a negligible change in the state of the ACS. When there is an evidence of a RW fault in the subsystem level, the probabilities corresponding to the RW states (component level) changes slightly despite the parameter variation. This indicates that the CDM is not sensitive to small variations in the network parameters, as desired.

7.4 V&V of the HFDM

In this thesis, by the term V&V of HFDM we imply the verification of fuzzy rule bases at different nodes of the HFDM. A fuzzy RBR system is usually constructed by encoding the observations of several human experts, and the experts may have observations and/or expertise that are in conflict with each other. Therefore, it

is necessary to validate the diagnostic knowledge that are encoded in one or more rule base(s). Rule bases that correspond to complex systems often consist of a large number of rules. The objective of rule base V&V is to ensure that there is no inconsistency or error in the rule base. The verification of rule-based systems becomes more important for rule bases that consist of a large number of rules.

Rule base verification has been investigated extensively in literature [160, 164, 165]. Formal verification of fuzzy rule bases are usually performed by utilizing petri-net models to check certain properties such as *redundancy*, *circularity*, *consistency*, and *completeness* of rules in a rule base. There is a systematic procedure in which rule bases are verified. The errors of interest are mainly the structural errors in the encoded rules. Such errors are related to redundancy (due to redundant and subsumed rules), circularity (due to infinite inference), inconsistency (due to conflicting rules), and incompleteness (due to missing rules) in the rule bases [160].

Note that the fuzzy rules that are utilized in the HFDM have a specific form as follows:

$$\text{If } (s_{p,1}^l \in M_{p,1,k}^l) \text{ and } (s_{p,2}^l \in M_{p,2,k}^l) \dots \text{ and } (s_{p,J}^l \in M_{p,J,k}^l) \text{ then } (f_k^l)$$

where $s_{p,j}^l$, $M_{p,j,k}^l$, and f_k^l have their usual meaning as mentioned in Chapter 5. Note that the set of faults $F_p^l = \{f_k : k = 1, \dots, K\}$, as specified in Chapter 5, corresponds to the possible health states $X_p^l = \{x_k : k = 1, \dots, K\}$ that are specified in Chapter 6. The following are true for the set of rules that are specified in a FDM (refer to Definition 5.2.3):

1. There is only one consequent (fault) for each rule, and all the possible values of the diagnostic signals that correspond to the consequent (fault) are specified in the antecedent part of the rule. Therefore, a “redundancy error” can occur in cases where either a rule is specified multiple times, or for a given consequent

(fault), there exists at least one rule that is subsumed into another rule.

2. The consequent part of a rule never appears in the antecedent part of another rule. Therefore, the possibility of any “circularity error” is ruled out.
3. Since there is only one consequent for each rule, an “inconsistency error” will not occur unless the antecedent parts of any two rules that correspond to two different consequents (faults) are the same.
4. The “incompleteness error” can occur either when there are no rule specified for a known fault (or health state) of the component, or there exists an unknown faulty state of the component.
5. Due to the hierarchical decomposition of our methodology the number of rules are few in numbers.

It is important to note that since the overall spacecraft formation flight is decomposed hierarchically, the fuzzy rules are specified separately (and in isolation) for each node in the proposed HFDM (refer to Chapter 5 for details). Faults that are under consideration in this thesis correspond to the RW nodes, the EPS nodes, and the Formation node as shown in Figure 5.4. One rule has been specified for a given fault at a node. Therefore, each of the rule bases that corresponds to one of the nodes consists of a few rules. Consequently, verification of the rule bases is somewhat trivial for the implemented HFDM due to the following reasons:

Redundancy: In the implemented HFDM, a single rule is specified for a given fault, and it is easy to verify that given consequent (fault), there exists no rule that is subsumed into another rule.

Circularity: As explained above, circularity error is ruled out because consequent part of a rule never appears in the antecedent part of another rule in the HFDM.

Inconsistency: One needs to ensure that the antecedent parts of any two rules that correspond to two different consequents (faults) are not the same. Consider the fault manifestations that are encoded in the fuzzy rules for diagnosing faults in the independent components at Level 1 (refer to Section 5.3). It is easily verifiable that antecedent parts of any two rules (diagnostic signal values for the friction fault and the current fault as well as the ones for identifying the healthy state) are not the same. The rules in the formation node as well as the ones in the electrical power subsystem (EPS) nodes are verified to be consistent as well.

Incompleteness: In this thesis, faults at some selected nodes of the HFDM have been considered, and one rule was specified for each of the faults under consideration. Furthermore, since all the faults under consideration were injected in a simulation model, there was no unknown faulty state. Therefore, any incompleteness error is ruled out.

Because of the above-mentioned reasons, verification of the implemented fuzzy rule-based HFDM is not investigated further in this thesis.

7.5 Summary

In this chapter, the validation of the Bayesian network-based fault diagnosis model namely, the CDM that was developed in Chapter 6 is investigated. A thorough analysis of the parameter variations in the CDM is provided. The parameter variations are induced by changes in the confusion matrix of a given node. It has been shown analytically that the behavior of $P(h|e)$ with respect to a varied parameter of interest θ can be expressed as a ratio of two polynomials of degree 3; where H is a hypothesis variable in the CDM, and h is a particular state of H which is the focus of interest. A number of sample CDM verification results are presented in the form of sensitivity plots which demonstrate that the implemented CDM is not sensitive

to small variations in the network parameters, as desired. The verification of the fuzzy rule-based fault diagnosis model namely, the HFDM that was developed in Chapter 5, is also discussed.

Chapter 8

Conclusions and Future Directions of Research

8.1 Concluding Remarks

In this thesis hierarchical fault diagnosis framework, models and algorithms have been developed to facilitate systematic and coherent diagnostic reasoning in complex systems such as a satellite formation flight system by decomposing its complex structure hierarchically into simpler modules or components. The decomposition is driven by the need, from project management perspective, for supporting the development of the components/subsystems of the overall system by a number of teams and by performing an integration at the end.

Hierarchical fault diagnosis in satellites formation flight has been investigated first by developing a fuzzy rule-based hierarchical fault diagnosis model (HFDM), which is then extended to a Bayesian network-based component dependency model (CDM) that is flexible to utilize fuzzy rule-based diagnosis at various nodes in the CDM. The fuzzy rule-based and the Bayesian network-based approaches were chosen so that appropriate modeling of fault behaviors can be performed which

would allow diagnostic decision making under uncertainty. The Verification and Validation (V&V) of the proposed models have also been investigated.

The proposed CDM-based scheme is found to have potential to serve as a fault diagnosis tool that can automate the tasks of the operators at ground stations. Such a fault diagnosis tool will be particularly useful to the less-experienced operators for performing the ground support-based health management tasks of a large number of satellites in a formation. Furthermore, though the development of our proposed methodology is based on the health management of satellites formation flight, the methodology is generic enough to be applicable to other systems or a fleet of systems that require health monitoring decision support systems (DSS).

8.2 Future Research Directions

One may pursue the following research directions to investigate further the fault diagnosis models and algorithms that are developed in this thesis.

8.2.1 Investigation of the CPT Generation

In this research the CDM parameters, namely the CPTs, are determined by computing some initial probability distributions and by computing the remaining distributions by using a weighted-sum of the initial distributions. The weights can be determined either by consulting the domain experts, or by developing a rigorous weight assignment policy (as discussed at the end of Section 6.2.3). One may investigate the development of a weight assignment policy that is based on prior probabilities of the faults in the initial distributions under consideration. However, in order to minimize biases towards certain types of faults that are frequently identified, the policy may include other considerations such as component operating hours since some faults may develop only toward the end of life of the component whereas

others may develop at the early stages. In addition, it would be a valuable research to validate the developed policy with the opinion of a domain expert.

8.2.2 Investigation of the Hierarchical Agreement Factor

As pointed out in Section 6.5, a limitation of the proposed CDM may be the *belief adjustment factor* that is used to quantify “hierarchical health state agreements” between the fault manifestations in two CDM nodes. In this thesis, the belief adjustment factor is defined as a ratio of two class accuracies. This may appear to be an over-simplification of the component dependency and fault manifestation mappings in real-world complex dynamical systems. Consequently, it would be necessary to find an alternative way of defining the belief adjustment factor. Such investigation may employ suitable estimation models which would be able to quantify the hierarchical health state agreements in two CDM nodes.

8.2.3 Investigation of the Dynamic CDM

The extension of the proposed CDM to a “dynamic CDM” will be an interesting research problem that may be pursued especially if data that is representative of the time progression of faults in the system is available. It is well-known that in general the more the severity of faults increases in a system over time, the better the performance of the diagnosis algorithms becomes. Consequently, the confusion matrices that are used to compute the CDM parameters would change over such time durations. Therefore, an interesting problem would be to develop a methodology that would facilitate the selection of appropriate confusion matrices that are based on the estimated fault severity. This investigation will also allow one to determine if the CDM approach can be extended to prognosis or failure prediction of various components in the system under consideration.

8.2.4 Experimental Validation

Upon the availability of a real formation flight mission telemetry data, investigations on the validation of the HFDM and/or the CDM with the actual telemetry data would be an interesting research that one may pursue. Such investigations will allow one to validate the independence assumptions on fault manifestations that are made while determining the CDM and the HFDM structures, as well as the CDM parameters (initial distributions).

8.2.5 The Cost-Benefit Analysis

An important research that is related to the proposed fault diagnosis methodologies is the cost-benefit analysis in a practical environment with real system data. There have been considerable interest in such investigations (for example, refer to [166] where the authors derives cost matrices from confusion matrices). Such analysis provides more realistic assessment of a diagnostic algorithm under the expected operating conditions, the cost of fault occurrences, and the mis-diagnosis that impacts the algorithms value.

Bibliography

- [1] B. J. Clement and A. C. Barrett, “Coordination Challenges for Autonomous Spacecraft,” in *AAMAS-02 Workshop Notes on Toward an Application Science: MAS Problem Spaces and Their Implications to Achieving Globally Coherent Behavior*, Italy, June 2002.
- [2] “Earth Observing System,” CloudSat Mission Webpage, Cited: May 2008. [Online]. Available: <http://cloudsat.atmos.colostate.edu/mission>
- [3] “Terrestrial Planet Finder,” NASA-JPL, Cited: May 2008. [Online]. Available: http://planetquest.jpl.nasa.gov/{TPF}/tpf_index.cfm
- [4] “Concept of Satellite Formation Flying Becoming a Reality,” NASA Goddard Space Flight Center, Cited: May 2008. [Online]. Available: <http://www.gsfc.nasa.gov/topstory/20010601eo1.html>
- [5] M. Zink, H. Fiedler, I. Hajnsek, G. Krieger, A. Moreira, and M. Werne, “The TanDEM-X Mission Concept,” in *Proc. 2006 IEEE International Geoscience and Remote Sensing Symposium*, July-August 2006, pp. 1938–1941.
- [6] E. Gill and H. Runge, “Tight Formation Flying for an Along-Track SAR Interferometer,” *Acta Astronautica*, vol. 55, pp. 473–485, 2004.
- [7] “Global Precipitation Measurement (GPM),” NASA Goddard Space Flight Center, Cited: May 2008. [Online]. Available: <http://gpm.gsfc.nasa.gov>
- [8] “Cluster Mission,” ESA Space Science, Cited: May 2008. [Online]. Available: <http://www.esa.int/science/cluster>
- [9] “Current GPS Constellation,” U.S. Naval Observatory GPS Home Page, Cited: May 2008. [Online]. Available: <http://tycho.usno.navy.mil/gpscurr.html>
- [10] “Precision Formation Flying,” NASA-JPL, Cited: May 2008. [Online]. Available: <http://dst.jpl.nasa.gov/>
- [11] “Lisa Mission,” ESA Space Science, Cited: May 2008. [Online]. Available: <http://www.esa.int/science/lisa>

- [12] “Darwin Mission,” ESA Space Science, Cited: May 2008. [Online]. Available: <http://www.esa.int/science/darwin>
- [13] F. H. Bauer, K. Hartman, D. Weidow, J. P. How, and F. Busse, “Enabling Spacecraft Formation Flying through Spaceborne GPS and Enhanced Automation Technologies,” in *Proc. 1999 ION-GPS Conference*, Nashville, TN, September 1999, pp. 369–383.
- [14] K. Keller, D. Wiegand, K. Swearingen, C. Reising, S. Black, A. Gillis, and M. Vandernoot, “An Architecture to Implement Integrated Vehicle Health Management Systems,” in *Proc. IEEE Systems Readiness Technology Conference (Autotestcon 2001)*, Valley Forge, PA, USA, August 2001, pp. 2–15.
- [15] D. E. Paris, L. C. Trevino, and M. D. Watson, “A Framework for Integration of IVHM Technologies for Intelligent Integration for Vehicle Management,” in *Proc. 2005 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2005.
- [16] W. Kahle and J. Miller, “The Practical Value of Health Management in Space Exploration Systems,” in *Proc. 2005 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2005.
- [17] K. Keller, A. Baldwin, S. Ofsthun, K. Swearingen, J. Vian, T. Wilmering, and Z. Williams, “Health Management Engineering Environment and Open Integration Platform,” in *Proc. 2007 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2007.
- [18] K. Keller, W. Majkowski, and K. Swearingen, “Integrating Health Management into Legacy Platforms,” in *Proc. 2009 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2009.
- [19] J. Korbicz, J. M. Koscieny, Z. Kowalczyk, and W. Cholewa, Eds., *Fault Diagnosis: Models, Artificial Intelligence, Applications*. Germany: Springer, 2004.
- [20] R. Isermann, “Model-based Fault Detection and Diagnosis—Status and Applications,” *Annual Reviews in Control*, vol. 29, pp. 71–85, 2005.
- [21] D. L. Iverson, “System Health Monitoring for Space Mission Operations,” in *Proc. 2008 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2008, pp. 1–8.
- [22] D. Bernard, G. Doraist, E. Gamble, B. Kanefskyt, J. Kurien, G. K. Man, W. Millart, N. Muscettola, P. Nayak, K. Rajant, N. Rouquette, B. Smith, W. Taylor, and Y. Tung, “Spacecraft Autonomy Flight Experience: The DS1 Remote Agent Experiment,” in *Proc. AIAA*, Albuquerque, NM, 1999.

- [23] B. Smith, W. Milla, J. Dunphy, Y. Tung, P. Nayak, E. Gamble, and M. Clark, "Validation and Verification of the Remote Agent for Spacecraft Autonomy," in *Proc. IEEE Aerospace Conference*, Big Sky, MT, March 1999, pp. 449–468.
- [24] N. Muscettola, P. P. Nayak, B. Pell, and B. C. Williams, "Remote Agent: To Boldly Go Where No AI System Has Gone Before," *Artificial Intelligence*, vol. 103, No. 1-2, pp. 5–47, August 1998.
- [25] B. C. Williams and P. P. Nayak, "A Model-based Approach to Reactive Self-Configuring Systems," in *Proc. AAAI-96*, Portland, Oregon, August 1996, pp. 971–978.
- [26] M. L. James and L. P. Dubon, "An Autonomous Diagnostic and Prognostic Monitoring System for NASA's Deep Space Network," in *Proc. IEEE Aerospace Conference*, Big Sky, MT, March 2000, pp. 403–414.
- [27] J. Kurien and M. D. R-Moreno, "Cost and Benefits of Model-based Diagnosis," in *Proc. 2008 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2008, pp. 1–14.
- [28] R. Gessner, B. Kusters, A. Hefler, R. Eilenberger, J. Hartmann, and M. Schmidt, "Hierarchical FDIR Concepts in S/C Systems," in *Proc. 8th International Conference on Space Operations (SpaceOps2004)*, Montreal, Canada, May 2004.
- [29] R. Kapadia, R. Gross, M. Walker, and M. Venkatesh, "Health Monitoring Assessment and Prognostics (HealthMAP) for Advanced Arresting Gear (AAG) System," in *Proc. Annual Conference of the PHM Society*, San Diego, California, USA, September-October 2009.
- [30] R. R. Yager, "On the Construction of Hierarchical Fuzzy Systems Models," *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, vol. 28, No. 1, pp. 55–66, February 1998.
- [31] A. Mohammadi-Idghamishi and S. Hashtrudi-Zad, "Hierarchical Fault Diagnosis: Application to an Ozone Plant," *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, vol. 37, No. 5, pp. 1040–1047, September 2007.
- [32] M. Blanke, M. Kinnaert, L. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, 2nd ed. Germany: Springer, 2006.
- [33] R. I. John and P. R. Innocent, "Modeling Uncertainty in Clinical Diagnosis Using Fuzzy logic," *IEEE Transactions on Systems, Man, and Cybernetics - PART B: Cybernetics*, vol. 35, No. 6, pp. 1340–1350, December 2005.
- [34] G. Huang and H. Uang, "Robust Adaptive PID Tracking Control Design for Uncertain Spacecraft Systems: A Fuzzy Approach," *IEEE Transactions on*

Aerospace and Electronic Systems, vol. 42, No. 4, pp. 1506–1514, October 2006.

- [35] R.-N. P. Singh and W. H. Bailey, “Fuzzy Logic Applications to Multisensor-Multitarget Correlation,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 33, No. 3, pp. 752–769, July 1997.
- [36] B. Ristic, “Target Identification Using Belief Functions and Implication Rules,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 41, No. 3, pp. 1097–1103, July 2005.
- [37] R. Ganguli, “Application of Fuzzy Logic for Fault Isolation of Jet Engines,” *Journal of Engineering for Gas Turbines and Power*, vol. 125, No. 3, pp. 617–623, July 2003.
- [38] W. Wang, “An Intelligent System for Machinery Condition Monitoring,” *IEEE Transactions on Fuzzy Systems*, vol. 16, No. 1, pp. 110–122, February 2008.
- [39] T. Yairi, Y. Kato, and K. Hori, “Fault Detection by Mining Association Rules from House-keeping Data,” in *Proc. International Symposium on Artificial Intelligence, Robotics and Automation in Space*, 2001.
- [40] R. Mackey, M. James, H. Park, and M. Zak, “BEAM: Technology for Autonomous Self-Analysis,” in *IEEE Aerospace Conference*, Big Sky, MT, March 2001, pp. 2989–3001.
- [41] W. Wang, “An Enhanced Diagnostic System for Gear System Monitoring,” *IEEE Transactions on Systems, Man, and Cybernetics - PART B: Cybernetics*, vol. 38, No. 1, pp. 102–112, February 2008.
- [42] H. A. Talebi, K. Khorasani, and S. Tafazoli, “A Recurrent Neural Network-Based Sensor and Actuator Fault Detection and Isolation for Nonlinear Systems with Application to the Satellite’s Attitude Control Subsystem,” *IEEE Transactions on Neural Networks*, vol. 20, No. 1, pp. 45–60, January 2009.
- [43] A. Joshi, V. Gavriloiu, A. Barua, A. Garabedian, P. Sinha, and K. Khorasani, “Intelligent and Learning-based Approaches for Health Monitoring and Fault Diagnosis of RADARSAT-1 Attitude Control System,” in *Proc. 2007 IEEE International Conference on Systems, Man and Cybernetics (SMC 2007)*, Montreal, Canada, October 2007.
- [44] I. A. Al-Zyoud and K. Khorasani, “Neural Network-based Actuator Fault Diagnosis for Attitude Control Subsystem of an Unmanned Space Vehicle,” in *Proc. IEEE International Joint Conference on Neural Networks (IJCNN-2006)*, Vancouver, Canada, July 2006.
- [45] Z. Q. Li, L. Ma, and K. Khorasani, “A Dynamic Neural Network-based Reaction Wheel Fault Diagnosis for Satellites,” in *Proc. IEEE International*

Joint Conference on Neural Networks (IJCNN-2006), Vancouver, Canada, July 2006.

- [46] A. Valdes and K. Khorasani, “A Pulsed Plasma Thruster Fault Detection and Isolation Strategy for Formation Flying of Satellites,” *Applied Soft Computing*, vol. doi:10.1016/j.asoc.2009.09.005, September 2009.
- [47] A. Barua, P. Sinha, and K. Khorasani, “A Diagnostic Tree Approach for Fault Cause Identification in the Attitude Control Subsystem of Satellites,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 45, No. 3, pp. 983–1002, July 2009.
- [48] N. Tudoroiu and K. Khorasani, “Satellite Fault Diagnosis using a Bank of Interactive Kalman Filters,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 43, No. 4, pp. 1334–1350, October 2007.
- [49] S. N. Huang, K. K. Tan, and T. H. Lee, “Automated Fault Detection and Diagnosis in Mechanical Systems,” *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, vol. 37, No. 6, pp. 1360–1364, November 2007.
- [50] X. Dai, Z. Gao, T. Breikin, and H. Wang, “Disturbance Attenuation in Fault Detection of Gas Turbine Engines: A Discrete Robust Observer Design,” *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, vol. 39, No. 2, pp. 234–239, March 2009.
- [51] W. Chen and M. Saif, “An Observer Based Fault Diagnosis of a Satellite System Subject to Time-varying Thruster Faults,” *ASME Journal of Dynamic Systems, Measurement and Control*, vol. 129, Issue 3, pp. 352–356, May 2007.
- [52] D. Nikovski, “Constructing Bayesian Networks for Medical Diagnosis from Incomplete and Partially Correct Statistics,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 12, No. 4, pp. 509–516, July/August 2000.
- [53] N. E. Fenton, M. Neil, and J. G. Caballero, “Using Ranked Nodes to Model Qualitative Judgments in Bayesian Networks,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, No. 10, pp. 1420–1432, October 2007.
- [54] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. San Monteo, CA, USA: Morgan Kaufmann, 1988.
- [55] F. V. Jensen and T. D. Nielsen, *Bayesian Networks and Decision Graphs*, 2nd ed. NY, USA: Springer, 2007.
- [56] “Health and Usage Monitoring Metrics, Monitoring the Monitor,” Society of Automotive Engineers (SAE) Standard, Issuing Committee: E-32 Aerospace Propulsion Systems Health Management, February 2008, Document No. ARP 5783.

- [57] D. L. Simon, J. W. Bird, C. R. Davison, A. Volponi, and R. E. Iverson, "Benchmarking Gas Path Diagnostic Methods: A Public Approach," in *Proc. 2008 ASME Turbo Expo Conference*, Berlin, Germany, May 2008.
- [58] X. Lau, A. S. Willisky, and G. C. Verghese, "Optimally Robust Redundancy Relations for Failure Detection in Uncertain systems," *Automatica*, vol. 22, No. 3, pp. 333–344, 1986.
- [59] R. J. Patton and J. Chen, "Review of Parity Space Approaches to Fault Diagnosis for Aerospace Systems," *Journal of Guidance, Control and Dynamics*, vol. 17, No. 2, pp. 278–285, March-April 1994.
- [60] J. Gertler, "Fault Detection and Isolation using Parity Relations," *Control Engineering Practice*, vol. 5, No. 5, p. 653661, 1997.
- [61] R. Isermann, "Process Fault Detection Based on Modeling and Estimation Methods – A Survey," *Automatica*, vol. 20, No. 4, pp. 387–404, 1984.
- [62] ———, "Fault Diagnosis of Machines via Parameter Estimation and Knowledge Processing – Tutorial Paper," *Automatica*, vol. 29, No. 4, pp. 815–835, 1993.
- [63] H. HanYong and S. ZengQi, "Fault Detection and Isolation of Flight Based on Robust Observer," in *Fifth World Congress on Intelligent Control and Automation (WCICA)*, Vol. 2, June 2004, pp. 1642–1645.
- [64] G. R. Duan and R. J. Patton, "Robust Fault Detection in Linear Systems using Luenberger Observers," in *UKACC International Conference on Control '98*, Swansea, UK, September 1998, pp. 1468–1473.
- [65] C. T. Chang and J. I. Hwang, "Simplification Techniques for EKF Computations in Fault Diagnosis – Suboptimal Gains," *Chemical Engineering Science*, vol. 53 (22), p. 38533862, 1998.
- [66] S. Grenaille, D. Henry, and A. Zolghadri, "Fault Diagnosis in Satellites using H-infinity Estimators," in *Proc. 2004 IEEE International Conference on Systems, Man and Cybernetics*, Volume 6, October 2004, pp. 5195–5200.
- [67] N. Tudoroiu and K. Khorasani, "Fault Detection and Diagnosis for Reaction Wheels of Satellites Attitude Control System using a Bank of Kalman Filters," in *Proc. International Symposium on Signals, Circuits and Systems*, Vol. 1, 2005, pp. 199–202.
- [68] R. Mohammadi, S. Hashtrudi-Zad, and K. Khorasani, "Hybrid Fault Diagnosis: Application to a Gas Turbine Engine," in *Proc. 2009 ASME Turbo Expo Conference*, Orlando, FL, USA, June 2009.
- [69] G. Biswas, "A Hierarchical Model-based Approach to Systems Health Management," in *Proc. 2007 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2007.

- [70] A. J. Weiner, D. A. Thurman, and C. M. Mitchell, "Applying Case-Based Reasoning to Aid Fault Management in Supervisory Control," in *Proc. 2005 IEEE International Conference on Systems, Man and Cybernetics*, Vancouver, British Columbia, Canada, October 1995, pp. 4213–4218.
- [71] A. Saxena, B. Wu, and G. Vachtsevanos, "Integrated Diagnosis and Prognosis Architecture for Fleet Vehicles using Dynamic Case Based Reasoning," in *Proc. the IEEE-Autotestcon*, Orlando, Florida, USA, September 2005, pp. 96–102.
- [72] K. K. Penta and D. Khemani, "Satellite Health Monitoring Using CBR Framework," in *Advances in Case-Based Reasoning*. Springer Berlin/Heidelberg, 2004, vol. 3155/2004, pp. 732–747.
- [73] C. M. Graichen and W. Cheetham, "Case-Based Reasoning Approaches for Gas Turbine Trip Diagnosis," in *Proc. 2007 ASME Turbo Expo Conference*, Montreal, Canada, May 2007.
- [74] Q. Xia and M. Rao, "Dynamic Case-Based Reasoning for Process Operation Support," *Engineering Applications of Artificial Intelligence*, vol. 12, p. 343361, 1999.
- [75] H. Berenji, Y. Wang, and A. Saxena, "Dynamic Case-Based Reasoning in Fault Diagnosis and Prognosis," in *Proc. 2005 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE'05)*, Reno, Nevada, USA, May 2005.
- [76] C. M. Fong and S. C. Hui, "An Intelligent Online Machine Fault Diagnosis System," *Computing and Control Engineering Journal*, vol. 12, Issue. 5, pp. 217–223, October 2001.
- [77] Y. L. Murphey, J. A. Crossman, Z. Chen, and J. Cardillo, "Automotive Fault Diagnosis - Part II: A Distributed Agent Diagnostic System," *IEEE Transactions on Vehicular Technology*, vol. 52, No. 4, July 2003.
- [78] A. Saxena, "Knowledge-Based Architecture for Integrated Condition Based Maintenance of Engineering Systems," PhD Dissertation, Georgia Institute of Technology, School of Electrical and Computer Engineering, August 2007.
- [79] U. M. Schwuttke, J. R. Veregge, and A. G. Quan, "Cooperating Expert Systems for the Next Generation of Real-time Monitoring Applications," in *Proc. 1994 International Conference on Expert Systems for Development*, March 1994, pp. 210–215.
- [80] D. Gayme, S. Menon, C. Ball, D. Mukavetz, and E. Nwadiogbu, "Fault Detection and Diagnosis in Turbine Engines using Fuzzy Logic," in *Proc. 22nd International Conference of the North American Fuzzy Information Processing Society*, Chicago, Illinois, USA, July 2003, pp. 341–346.

- [81] E. Applebaum, “Fuzzy Classification for Fault Isolation in Gas Turbine Engines,” in *Proc. Joint 9th IFSA World Congress and 20th NAFIPS International Conference*, Vancouver, BC, Canada, July 2001, pp. 292–297.
- [82] R. Milne and C. Nicol, “TIGER: A Model Based and Rule Based Real-Time Tool for Monitoring and Diagnosis of Dynamic Systems,” in *Proc. IEE Colloquium on Real-Time Knowledge Based Systems*, January 1995, pp. 8/1–8/4.
- [83] D. Cayrac, D. Dubois, and H. Prade, “Handling Uncertainty with Possibility Theory and Fuzzy Sets in a Satellite Fault Diagnosis Application,” *IEEE Transactions on Fuzzy Systems*, vol. 4, No. 3, 1996.
- [84] J. M. Koscieny and M. Syfert, “Fuzzy Diagnostic Reasoning that Takes into Account the Uncertainty of the Relation between Faults and Symptoms,” *International Journal of Applied Mathematics and Computer Science*, vol. 16, No.1, pp. 27–35, 2006.
- [85] J. M. Koscieny, M. Bartys, and M. Syfert, “The Practical Problems of Fault Isolation in Large Scale Industrial Systems,” in *Proc. 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (Safeprocess2006)*, Beijing, P. R. China, August-September 2006.
- [86] M. A. El-Gamal and M. Abdulghafour, “Fault Isolation in Analog Circuits using a Fuzzy Inference System,” *Computers and Electrical Engineering*, vol. 29, No. 1, pp. 213–229, January 2003.
- [87] S. Yu, Z. Hai, S. Wei-Ji, W. Gang, and Z. Xiao-Dan, “Fuzzy Reasoning Based Fault Diagnosis Expert System,” in *Proc. 2004 IEEE International Conference on Networking, Sensing and Control*, March 2004, pp. 613–617.
- [88] M. A. El-Gamal and M. Abdulghafour, “Application of a Novel Fuzzy Classifier to Fault Detection and Isolation of the DAMADICS Benchmark Problem,” *Control Engineering Practice*, vol. 14, No. 6, pp. 653–669, June 2006.
- [89] B. Yan, T. Zhang, and C. Xie, “Fuzzy Expert System for Fault Diagnosis of Robotic Assembly,” in *Proc. 4th World Congress on Intelligent Control and Automation*, Shanghai, China, June 2002, pp. 445–449.
- [90] D. Juricic, A. Znidarsic, and D. Fussel, “Generation of Diagnostic Trees by Means of Simplified Process Models and Machine Learning,” *Engineering Applications of Artificial Intelligence*, vol. 10, No. 1, pp. 15–29, February 1997.
- [91] W. Sun, J. Chen, and J. Li, “Decision Tree and PCA-based Fault Diagnosis of Rotating Machinery,” *Mechanical Systems and Signal Processing*, vol. 21, Issue 3, pp. 1300–1317, April 2007.
- [92] M. Schwabacher, R. Aguilar, and F. Figueroa, “Using Decision Trees to Detect and Isolate Simulated Leaks in the J-2X Rocket Engine,” in *Proc. 2009 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2009.

- [93] C. A. Ericson, "Fault Tree Analysis – A History," in *Proc. 17th International System Safety Conference*, Florida, USA, August 1999.
- [94] W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, "Fault Tree Handbook with Aerospace Applications," NASA Office of Safety And Mission Assurance, NASA Headquarters, Washington, DC 20546, Tech. Rep. Version 1.1, August 2002.
- [95] C. Lee, R. L. Alena, and P. Robinson, "Migrating Fault Trees to Decision Trees for Real Time Fault Detection on International Space Station," in *Proc. 2005 IEEE Aerospace Conference*, Bigsky, Montana, March 2005, pp. 1–6.
- [96] T. Yairi, M. Nakatsugawa, K. Hori, S. Nakasuka, K. Machida, and N. Ishihama, "Adaptive Limit Checking for Spacecraft Telemetry Data Using Regression Tree Learning," in *Proc. 2004 IEEE International Conference on Systems, Man and Cybernetics*, The Hague, The Netherlands, October 2004, pp. 5130–5135.
- [97] D. Fuessel and R. Isermann, "Hierarchical Motor Diagnosis Utilizing Structural Knowledge and a Self-Learning Neuro-Fuzzy Scheme," *IEEE Transactions on Industrial Electronics*, vol. 47, Issue. 5, pp. 1070–1077, October 2000.
- [98] A. Khosravi, H. A. Talebi, and M. Karrari, "Fault Detection and Isolation for Unknown Nonlinear Systems Using Expert Methods," in *Proc. 2005 IEEE International Conference on Control Applications (CCA-2005)*, Toronto, Canada, August 2005, pp. 1485–1490.
- [99] J. Calado, J. S. da Costa, M. Bartys, and J. Korbicz, "FDI Approach to the DAMADICS Benchmark Problem Based on Qualitative Reasoning Coupled with Fuzzy Neural Networks," *Control Engineering Practice*, vol. 14, No. 6, pp. 685–698, June 2006.
- [100] R. Davis, "Diagnostic Reasoning Based on Structure and Behavior," *Artificial Intelligence*, vol. 24, Issue 1-3, pp. 347–410, December 1984.
- [101] A. Ligeza and P. Fuster-Parra, "A Multi-Level Knowledge-Based Model of Diagnostic Reasoning," in *Information Modelling and Knowledge Bases IX*, P. J. Charrel, Ed. IOS Press, Tuluza, France, 1998, pp. 330–344.
- [102] K. Zhao and B. R. Upadhyaya, "Adaptive Fuzzy Inference Causal Graph Approach to Fault Detection and Isolation of Field Devices in Nuclear Power Plants," *Progress in Nuclear Energy*, vol. 26, No. 3-4, pp. 226–240, 2005.
- [103] M. J. Daigle, X. D. Koutsoukos, and G. Biswas, "Distributed Diagnosis in Formations of Mobile Robots," *IEEE Transactions on Robotics*, vol. 23, Issue 2, pp. 353–369, April 2007.

- [104] O. Erdinc, C. Brideau, P. Willett, and T. Kirubarajan, "Fast Diagnosis with Sensors of Uncertain Quality," *IEEE Transactions on Systems, Man and Cybernetics - Part B: Cybernetics*, vol. 38, Issue 4, pp. 1157–1165, August 2008.
- [105] M. Paako and P. Myllymaki, "Bayesian Networks for Advanced FDIR," in *ESA Workshop on On-Board Autonomy*, Noordwijk, The Netherlands, October 2001.
- [106] Y. Kawahara, R. Fujimaki, T. Yairi, and K. Machida, "Diagnosis Method for Spacecraft using Dynamic Bayesian Networks," in *Proc. 8th International Symposium on Artificial Intelligence, Robotics and Automation in Space*, B. Battrick, Ed. European Space Agency, 2005.
- [107] B. M. Sanchez and P. H. Ibarngoytia, "Online Diagnosis using Influence Diagrams," in *Advances in Artificial Intelligence*. Springer Berlin/Heidelberg, 2004, vol. 2972/2004, pp. 546–554.
- [108] K. W. Przytula and D. Thompson, "Construction of Bayesian Networks for Diagnostics," in *Proc. 2000 IEEE Aerospace Conference*, Big Sky, MT, USA, March 2000, pp. 193–200.
- [109] K. W. Przytula, G. B. Isdale, and T.-C. Lu, "Collaborative Development of Large Bayesian Networks," in *Proc. 2006 IEEE AUTOTESTCON*, Anaheim, CA, USA, 2006, pp. 515–522.
- [110] K. W. Przytula and A. Choi, "An Implementation of Prognosis with Dynamic Bayesian Networks," in *Proc. 2008 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2008.
- [111] B. Saha and K. Goebel, "Uncertainty Management for Diagnostics and Prognostics of Batteries using Bayesian Techniques," in *Proc. 2008 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2008.
- [112] H. Tu, J. Allanach, S. Singh, K. R. Pattipati, and P. Willett, "Information Integration via Hierarchical and Hybrid Bayesian Networks," *IEEE Transactions on Systems, Man and Cybernetics, Part A*, vol. 36, Issue. 1, pp. 19–33, January 2006.
- [113] Y. Zhang and K.-J. Lin, "Hierarchical management of service accountability in service oriented architectures," in *Proc. 2007 IEEE International Conference on Service-Oriented Computing and Applications (SOCA '07)*, June 2007, pp. 55–64.
- [114] D. E. Bernard, G. A. Dorais, C. Fry, E. B. G. Jr., B. Kanefsky, J. Kurien, W. Millar, N. Muscettola, P. P. Nayak, B. Pell, K. Rajan, N. Rouquette, B. Smith, and B. C. Williams, "Design of the Remote Agent Experiment for Spacecraft Autonomy," in *Proc. 1998 IEEE Aerospace Conference*, March 1998, pp. 259–281.

- [115] S. H. Chung and A. Barrett, “Distributed Real-time Model-based Diagnosis,” in *IEEE Aerospace Conference*, Big Sky, MT, March 2003, pp. 1.349–1.355.
- [116] A. Guiotto, A. Martelli, and C. Paccagnini, “SMART-FDIR: Use of Artificial Intelligence in the Implementation of a Satellite FDIR,” in *ESA SP-532: DASIA 2003*, 2003.
- [117] W. E. Vesley, F. F. Goldberg, and N. H. Roberts, “Fault Detection, Isolation and Recovery (FDIR) in On-Board Software,” Chalmers University of Technology, Goteborg, Sweden, Tech. Rep. Master’s Thesis, 2005.
- [118] M. A. Swartwout, “A Systematic formulation of Spacecraft Health Management Decisions,” in *IEEE Aerospace Conference*, Big Sky, MT, March 2001, pp. 7.3393–7.3405.
- [119] T. Kurtoglu, D. Jensen, and S. Poll, “Systematic Benchmarking of Diagnostic Technologies for an Electrical Power System,” in *Proc. 2009 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2009.
- [120] A. Saxena, J. Celaya, and B. Saha, “Evaluating Algorithm Performance Metrics Tailored for Prognostics,” in *Proc. 2009 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2009.
- [121] H. J. Zimmermann, *Fuzzy Set Theory - and Its Applications*, 4th ed. USA: Kluwer Academic Publishers, 2001.
- [122] F. Jensen, *An Introduction to Bayesian Networks*. London: UCL Press, 1996.
- [123] B. Bialke, “High Fidelity Mathematical Modeling of Reaction Wheel Performance,” *Advances in the Astronautical Sciences*, vol. 98, pp. 483–496, 1998.
- [124] Z. Jiang, S. Liu, and R. A. Dougal, “Design and Testing of Spacecraft Power Systems Using VTB,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, No. 3, pp. 976–989, July 2003.
- [125] “Satellite Electrical Power System,” USC Virtual Test Bed Homepage, Cited: July 2009. [Online]. Available: <http://vtb.ee.sc.edu/applications/>
- [126] C. Lenz, “Close Range Formation Flight in Low Earth Orbit for Synthetic/Sparse Aperture Earth Imaging Missions,” Colorado Center for Astrodynamics Research Home Page, Cited: March 2008. [Online]. Available: http://ccar.colorado.edu/asen5050/projects/projects_2000/lenz
- [127] G. W. Hill, “Researches in Luner Theory,” *American Journal of Mathematics*, vol. 1, No. 1, pp. 5–26, 1878.
- [128] S. R. Vadali, S. S. Vaddi, and K. T. Alfriend, “An Intelligent Control Concept for Formation Flying Satellites,” *International Journal of Robust and Nonlinear Control*, vol. 12, pp. 97–115, 2002.

- [129] G. Krieger, A. Moreira, H. Fiedler, I. Hajnsek, M. Werner, M. Younis, and M. Zink, "TanDEM-X: A Satellite Formation for High-Resolution SAR Interferometry," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 45, No. 11, pp. 3317–3341, November 2007.
- [130] B. Wie, *Space Vehicle Dynamics and Control*. Virginia, USA: AIAA Inc., 1998.
- [131] G. Yang, Q. Yang, V. Kapila, D. Palmer, and R. Vaidyanathan, "Fuel Optimal Manoeuvres for Multiple Spacecraft Formation Reconfiguration using Multi-Agent Optimization," *International Journal of Robust and Nonlinear Control*, vol. 12, pp. 243–283, 2002.
- [132] "Satellite Classification," Small Satellites Home Page, Cited: March 2008. [Online]. Available: http://centaur.sstl.co.uk/SSHP/sshp_classify.html
- [133] P. C. Hughes, *Spacecraft Attitude Dynamics*. USA: John Wiley & Sons Inc., 1986.
- [134] W. Ren and R. W. Beard, "Decentralized Scheme for Spacecraft Formation Flying via the Virtual Structure Approach," *AIAA Journal of Guidance, Control and Dynamics*, vol. 27, No. 1, pp. 73–82, January 2004.
- [135] B. C. Kuo, *Automatic Control Systems*, 7th ed. Prentice-Hall Inc., 1995.
- [136] K. Ogata, *Modern Control Engineering*, 3rd ed. N.J., USA: Prentice-Hall Inc., 1996.
- [137] J. R. Wertz and W. J. Larson, Eds., *Space Mission Analysis and Design*. USA: Kluwer Academic Publishers, 1999.
- [138] Z. Jiang, R. A. Dougal, and S. Liu, "Application of VTB in Design and Testing of Satellite Electrical Power Systems," *Journal of Power Sources*, vol. 122, pp. 95–108, 2003.
- [139] M. E. Pittelkau, "Definitions, Metrics, and Algorithms for Displacement, Jitter, and Stability," Flight Dynamics Analysis Branch (FDAB), NASA Goddard Space Flight Center, Cited: February 2008. [Online]. Available: http://geons.gsfc.nasa.gov/live/Home/Conf/&Symp_Papers.html
- [140] A. Barua and K. Khorasani, "Intelligent Model-based Hierarchical Fault Diagnosis for Satellite Formations," in *Proc. 2007 IEEE International Conference on Systems, Man and Cybernetics (SMC 2007)*, Montreal, Canada, October 2007.
- [141] B. Pell, D. E. Bernard, S. A. Chien, E. Gat, N. M. Muscettola, P. P. Nayak, M. D. Wagner, and B. C. Williams, "An Autonomous Spacecraft Agent Prototype," in *Autonomous Robots 5*. Kluwer Academic Publishers, 1998, pp. 29–52.

- [142] D. P. Watson and D. H. Scheidt, “Autonomous Systems,” *John Hopkins APL Technical Digest*, vol. 26, No. 4, pp. 368–376, 2005.
- [143] A. Barua and K. Khorasani, “A Hierarchical Fault Diagnosis and Fuzzy Rule-Based Reasoning for Satellites Formation Flight,” *Accepted for publication in IEEE Transactions on Aerospace and Electronic Systems*, 2010.
- [144] “Class Confusion Matrix,” LingPipe Home Page, Cited: June 2009. [Online]. Available: <http://alias-i.com/lingpipe/docs/api/com/aliasi/classify/ConfusionMatrix.html>
- [145] S. Renooij, “Probability Elicitation for Belief Networks: Issues to Consider,” *The Knowledge Engineering Review*, vol. 163, No. 3, pp. 255–269, 2000.
- [146] L. C. V. D. Gaag, S. Renooij, C. L. M. Witteman, B. M. P. Aleman, and B. G. Taal, “How to Elicit Many Probabilities,” in *Proc. 15th Annual Conference on Uncertainty in Artificial Intelligence*, Stockholm, Sweden, August 1999, pp. 647–654.
- [147] J. V. Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, 3rd ed. ISBN: 0471911852: John Wiley & Sons Inc., 1953.
- [148] D. V. Winterfeldt and W. Edwards, *Decision Analysis and Behavioral Research*, 1st ed. ISBN: 0521273048: Cambridge University Press, 1986.
- [149] A. Barua and K. Khorasani, “Hierarchical Fault Diagnosis and Health Monitoring in Satellites Formation Flight,” *Accepted for publication in IEEE Transactions on Systems, Man, and Cybernetics - PART C: Applications and Reviews*, 2010.
- [150] M. Bednarskia, W. Cholewa, and W. Frid, “Identification of Sensitivities in Bayesian Networks,” *Engineering Applications of Artificial Intelligence*, vol. 17, pp. 327–335, 2004.
- [151] T. Kurtoglu, O. J. Mengshoel, and S. Poll, “A Framework for Systematic Benchmarking of Monitoring and Diagnostic System,” in *Proc. 2008 International Conference on Prognostics and Health Management*, Denver, Colorado, USA, October 2008.
- [152] K. B. Laskey and S. M. Mahoney, “Network Engineering for Agile Belief Network Models,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 12, No. 4, pp. 487–498, July/August 2000.
- [153] D. Kahneman, P. Slovic, and A. Tversky, “Judgment Under Uncertainty: Heuristics and Biases,” in *Judgment Under Uncertainty: Heuristics and Biases*, D. Kahneman, P. Slovic, and A. Tversky, Eds. Cambridge University Press, Cambridge, 1982, pp. 3–20.

- [154] A. Barua and K. Khorasani, "Hierarchical Fault Diagnosis and Health Monitoring in Multi-platform Space Systems," in *Proc. 2009 IEEE Aerospace Conference*, Big Sky, Montana, USA, March 2009.
- [155] "SAMIAM," Automated Reasoning Group, UCLA, Cited: July 2009. [Online]. Available: <http://reasoning.cs.ucla.edu/samiam/>
- [156] T. Menzies and C. Pecheur, "Verification and Validation and Artificial Intelligence," *Advances in Computers*, vol. 65, pp. 154–203, 2005.
- [157] S. A. Brown and C. Pecheur, "Model-Based Verification of Diagnostic Systems," NASA Marshall Space Flight Center, Tech. Rep. 20020073810, April 2002.
- [158] F. Cornelissen, C. Jonker, and J. Treur, "Compositional Verification of Knowledge-Based Systems: A Case Study in Diagnostic Reasoning," in *Knowledge Acquisition, Modelling and Management, Proc. of the 10th EKAW'97*, E. Plaza and R. Benjamins, Eds. Springer Verlag, 1997, vol. 1319, pp. 65–80.
- [159] F. Harmelen and A. Teije, "Validation and Verification of Conceptual Models of Diagnosis," in *Proc. 4th European Symposium on the Validation and Verification of Knowledge Based Systems (EUROVAV97)*, Leuven, Belgium, 1997, pp. 117–128.
- [160] S. Yang, J. Tsai, and C. Chen, "Fuzzy Rule Base Systems Verification Using High-Level Petri Nets," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, No. 2, pp. 457–473, March–April 2003.
- [161] H. Wang, "Using Sensitivity Analysis to Validate Bayesian Networks for Airplane Subsystem Diagnosis," in *Proc. 2006 IEEE Aerospace Conference*, Big Sky, MT, USA, March 2006.
- [162] B. Guo, "Verifying Parameters of Bayesian Belief Networks by Exploring the Impact Intensity," in *Proc. 2005 IEEE International Conference on Natural Language Processing and Knowledge Engineering (IEEE NLP-KE'05)*, October–November 2005, pp. 723–728.
- [163] E. Santos, "Verification and Validation of Bayesian Knowledge-Bases," *Data and Knowledge Engineering*, vol. 37, pp. 307–329, 2001.
- [164] S. Viaene, G. Wets, and J. Vanthienen, "A Synthesis of Fuzzy Rule-based System Verification," *Fuzzy Sets and Systems*, vol. 113, Issue 2, pp. 253–265, July 2000.
- [165] L. Fei, Y. Ming, and S. Peng, "Verification and Validation of Fuzzy Rules-based Human Behavior Models," in *Proc. 7th International Conference on System Simulation and Scientific Computing*, Beijing, China, October 2008, pp. 813–819.

- [166] C. R. Davison and C. Drummond, "Application of Cost Matrices and Cost Curves to Enhance Diagnostic Health Management Metrics for Gas Turbine Engines," in *Proc. 2009 ASME Turbo Expo Conference*, Orlando, FL, USA, June 2009.