

Asset Analytics

Performance and Safety Management

*Series Editors: Ajit Kumar Verma · P. K. Kapur · Uday Kumar*

Raj Kamal Kaur

Lalit Kumar Singh

Pooja Singh

Ajit K. Verma

# Security Management for Industrial Safety Critical Applications

A Practical Approach

 Springer

# **Asset Analytics**

## **Performance and Safety Management**

### **Series Editors**

Ajit Kumar Verma, Western Norway University of Applied Sciences, Haugesund, Rogaland Fylke, Norway

P. K. Kapur, Centre for Interdisciplinary Research, Amity University, Noida, India

Uday Kumar, Division of Operation and Maintenance Engineering, Luleå University of Technology, Luleå, Sweden

The main aim of this book series is to provide a floor for researchers, industries, asset managers, government policy makers and infrastructure operators to cooperate and collaborate among themselves to improve the performance and safety of the assets with maximum return on assets and improved utilization for the benefit of society and the environment.

Assets can be defined as any resource that will create value to the business. Assets include physical (railway, road, buildings, industrial etc.), human, and intangible assets (software, data etc.). The scope of the book series will be but not limited to:

- Optimization, modelling and analysis of assets
- Application of RAMS to the system of systems
- Interdisciplinary and multidisciplinary research to deal with sustainability issues
- Application of advanced analytics for improvement of systems
- Application of computational intelligence, IT and software systems for decisions
- Interdisciplinary approach to performance management
- Integrated approach to system efficiency and effectiveness
- Life cycle management of the assets
- Integrated risk, hazard, vulnerability analysis and assurance management
- Adaptability of the systems to the usage and environment
- Integration of data-information-knowledge for decision support
- Production rate enhancement with best practices
- Optimization of renewable and non-renewable energy resources

### **Review Process**

The proposal for each volume follows multi-pronged review process. The first level of review (single blind) is conducted by the series editors who may or may not decide to enlist the help of editorial board members for a second level of review. Proposals may also undergo a third level of peer review (double blind) if recommended by the Series Editors.

The series follows Ethics Statement found in the Springer standard guidelines here. <https://www.springer.com/us/authors-editors/journal-author/journal-author-helpdesk/before-you-start/before-you-start/1330#c14214>

Raj Kamal Kaur · Lalit Kumar Singh ·  
Pooja Singh · Ajit K. Verma

# Security Management for Industrial Safety Critical Applications

A Practical Approach

 Springer

Raj Kamal Kaur  
School of Computational Science  
GNA University  
Phagwara, Punjab, India

Pooja Singh  
Department of Mathematics  
SIES Graduate School of Technology  
Navi Mumbai, Maharashtra, India

Lalit Kumar Singh  
Research and Development  
Department of Atomic Energy  
NPCIL, Government of India  
Mumbai, Maharashtra, India

Ajit K. Verma  
Technical Safety  
Western Norway University of Applied  
Sciences  
Haugesund, Norway

ISSN 2522-5162

Asset Analytics

ISBN 978-981-97-4017-8

<https://doi.org/10.1007/978-981-97-4018-5>

ISSN 2522-5170 (electronic)

ISBN 978-981-97-4018-5 (eBook)

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

If disposing of this product, please recycle the paper.

# Preface

In the present scenario, the rapid adoption of e-technology is being used rapidly across all industrial and societal sectors. As a result, various digital technologies (such as electrical power, telecommunications, transportation, and avionics) have been deployed to meet human needs. However, these smart technologies are vulnerable to cyberattacks that compromise the system dependability. Such systems can fail catastrophically, causing significant harm both human and the natural world. Example include transportation accidents, Hatch Nuclear Station, emergency shutdown, and medical device failure due to a software failure will result in financial and human losses. As cybercrime and technological advancements continue to evolve, it is very important to evaluate the security metric of Safety-Critical Systems (SCSs) from the initial phase.

In this book, we present the concepts related to the security analysis of industrial safety-critical applications across seven chapters. Chapter 1 introduces the dependability metrics of SCS and the importance of security metric in dependability analysis. The basic principles for a Safety-Critical System are outlined in Chap. 2 while Chap. 3 presents important aspects of Cybersecurity. Chapter 4 provides the mathematical background necessary for understanding key security metrics in the analysis of SCS. The aim of Chap. 5 is to demonstrate insight and scope of analytical security analysis techniques. Chapter 6 presents the comparative study of dependability analytical models. Finally, Chap. 7 concludes this book.

Phagwara, India  
Mumbai, India  
Navi Mumbai, India  
Haugesund, Norway

Raj Kamal Kaur  
Lalit Kumar Singh  
Pooja Singh  
Ajit K. Verma

# Roadmap of Book

## Chapter 1 Dependability and Security

This chapter starts with the overview of the dependability metric. Furthermore, an attempt has been made to emphasize the significance of security metric in relation to other dependability measures. We point out the important motivation factors for conducting this research.

## Chapter 2 Fundamentals of Safety–Critical Systems

This chapter illustrates an outline of critical systems. In addition, it presents the structure and applications of safety-critical system. The challenges and open issues of SCSs are also included in this chapter.

## Chapter 3 Important Aspects of Cybersecurity

This chapter describes the cyberworld, cyberoperations, cyberweapons, and society’s critical infrastructure as targets in terms of cyberwarfare. In addition, definitions and domains of cybersecurity are explained in detail.

## Chapter 4 Mathematical Background

The second objective of the book is discussed in this chapter. This chapter contains two sections. In the first section, the important metrics of the security analysis of SCS are introduced. In the second section, the fundamental concepts of the random experiment, sample space, and events are presented.

## Chapter 5 Security Analysis Models

The evaluation of the security of software, the theme of the book, is necessarily carried out with the help of software models. As a result, practitioners have the knowledge about scheme that support dependability analysis modeling. This chapter focuses on the insights and scope of security analysis techniques. Limits and complementarity between techniques are also taken into account.

To illustrate the uses of these methodologies and help the reader to comprehend how the models are build, we employed different case examples.

## Chapter 6 Comparative Study of Analytical Models

Once the dependability (security) analysis process of SCSs has been achieved, further discussion about the concluding terms is illustrated in Chap. 7.

## Chapter 7 Conclusion

This chapter concludes this book.

Overall, this book is a sound research contribution to the security analysis of SCSs and puts the base for new efforts in this challenging scientific field. It will be important in the next research generation.



# Goal of Book

This book presents a holistic view of the process of security analysis of safety-critical safety and control systems.

The main specific objectives are:

1. Elaborate the needs for the security analysis of the SCSs.
2. Demonstrate the important terminologies used in the security analysis of the SCSs.
3. Demonstrate security analysis in practice with mathematical techniques using real-world case studies.
4. To demonstrate how each analytical approach may be used in the security analysis of SCSs, we compare analytical techniques using different cases.

# About This Book

This book is a scholarly book that can be read by students, researchers, policy-makers, and regulatory bodies interested in cybersecurity. The book also presents the subject of destination marketing to students and future practitioners in a structured way. It is primarily intended for students researching cybersecurity and securing information systems.

It can serve as a benchmark for undergraduate and graduate studies in cybersecurity. The book is written in simple language so that a reader without previous experience in the field will find it readable and understandable. Based on this expectation, we anticipate that each library will be interested in compiling extensions of this book.

# Contents

<b>1 Dependability and Security</b> .....	1
1.1 Introduction .....	1
1.2 Dependability .....	2
1.2.1 Importance of Security Vis-à-Vis Other Dependability Metrics .....	3
1.3 Fault-Error-Failure Pathology .....	7
1.4 Means to Attain Dependability .....	12
References .....	15
<b>2 Fundamentals of Safety–Critical Systems</b> .....	17
2.1 Introduction .....	17
2.2 Critical System .....	18
2.2.1 Types of Critical System .....	18
2.3 Safety–Critical System .....	20
2.4 Structure of Safety–Critical System .....	20
2.5 Important Concept Related to Safety–Critical System .....	24
2.6 Application Areas of SCSS .....	27
2.7 Accidents .....	34
2.8 Need of Analysis Approaches for Safety–Critical System .....	34
2.9 Challenges .....	36
References .....	38
<b>3 Important Aspects of Cybersecurity</b> .....	39
3.1 What Does “Cyber” Mean? .....	39
3.1.1 Drivers of Change in the Cyberworld .....	40
3.2 The Cybersecurity Landscape .....	41
3.2.1 Vulnerabilities .....	42
3.2.2 Cyberthreat .....	48
3.2.3 Attacks .....	52
3.3 Critical Infrastructure .....	59
3.3.1 SCADA .....	59
3.3.2 Distributed Control System (DCS) .....	61

- 3.3.3 Remote Terminal Unit ..... 63
- 3.3.4 Programmable Logic Controller (PLC) ..... 64
- 3.4 Cybersecurity and Its Domains ..... 66
  - 3.4.1 Types of Cybersecurity ..... 66
- 3.5 Standards ..... 69
- References ..... 81
- 4 Mathematical Background ..... 83**
  - 4.1 Metrics ..... 83
    - 4.1.1 Confidentiality ..... 85
    - 4.1.2 Accountability ..... 86
    - 4.1.3 Authorization ..... 86
    - 4.1.4 Integrity ..... 86
    - 4.1.5 Availability ..... 87
    - 4.1.6 Non-repudiation ..... 89
    - 4.1.7 Authentication ..... 90
  - 4.2 Mathematical Concepts ..... 94
    - 4.2.1 Random Experiment ..... 95
    - 4.2.2 Sample Space ..... 95
    - 4.2.3 Event ..... 96
    - 4.2.4 Combination of Events ..... 97
    - 4.2.5 Probability ..... 100
  - References ..... 106
- 5 Security Analysis Models ..... 107**
  - 5.1 Introduction ..... 107
  - 5.2 Analytical Evaluation ..... 108
    - 5.2.1 Model-Based Evaluation of the System Security ..... 108
  - References ..... 151
- 6 Comparative Study of Analytical Models ..... 153**
  - 6.1 Comparison Terms ..... 153
    - 6.1.1 Feasibility ..... 153
    - 6.1.2 Purpose of the Analysis ..... 154
    - 6.1.3 Top-Down and Bottom-Up ..... 154
    - 6.1.4 Inductive and Deductive ..... 155
    - 6.1.5 Cause Consequence Relationship ..... 155
    - 6.1.6 Accident Scenario ..... 156
    - 6.1.7 Single Point Failure and Multiple Point Failure ..... 156
    - 6.1.8 Qualitative and Quantitative ..... 156
    - 6.1.9 Static and Dynamic Models ..... 157
  - 6.2 Comparison on the Basis of Actions Performed Due  
to the Analysis Process ..... 157
    - 6.2.1 FTA ..... 157
    - 6.2.2 ETA Analysis Procedure ..... 161
    - 6.2.3 Markov Model Analysis Process ..... 163

- 6.2.4 Petri Nets Analysis Procedure ..... 164
- 6.2.5 Ordinary Differential Equations (ODE) Creation ..... 168
- 6.2.6 HAZOP Analysis Procedure ..... 173
- 6.2.7 Analysis Procedure of SWIFT ..... 175
- 6.2.8 Reliability Block Diagram Analysis Procedure ..... 179
- 6.2.9 FMEA Analysis Procedure ..... 184
- 6.2.10 FMECA ..... 185
- 6.2.11 Scenario Graph Analysis Procedure ..... 190
- 6.2.12 Analysis Procedure of Functional Failure Analysis  
(FFA) ..... 192
- 6.2.13 Attack Tree ..... 194
- 6.2.14 Markov Model ..... 197
- 6.3 Compare Techniques on the Basis of Result ..... 206
- References ..... 206
- 7 Conclusion ..... 209**
  - 7.1 Contributions and Summary of the Book ..... 209
  - 7.2 Future Scope of the Topic ..... 211

## About the Authors

**Raj Kamal Kaur** completed her Ph.D. from Lovely Professional University in Punjab, India in 2020. Currently, she is serving as an assistant professor at GNA University in Phagwara, Punjab, India. She has numerous publications in SCI-indexed international journals and conferences. She is also a reviewer of several reputable journals.

**Lalit Kumar Singh** received his Ph.D. degree from the Indian Institute of Technology (Banaras Hindu University). He is currently a Scientist in NPCIL-BARC, Department of Atomic Energy, Government of India, and has the distinction of working on Pressurized Heavy Water Reactors (PHWR) and Light Water Reactors (LWR). He has an illustrious career and succeeded in several critical jobs assigned to him in his illustrious career, though, each of them was challenging. His assignments over the years range from design, development, testing, IV&V, related research, and site validation of the safety-critical computer-based systems of Indian Nuclear Power Plants. He has published several research papers in journals of high impact factor such as IEEE Transactions, etc. He has been invited as chief guest, with keynote speeches, session chair, and talks at many international conferences, short-term courses, workshops and faculty development programs from many IITs, NITs and other institutes of national importance. He is supervising many Ph.D. theses from different IITs. He is an adjunct faculty in IITs, NITs and IIITs. He is a Senior Member of IEEE and a recipient of many awards like publication awards, group achievement awards, etc. He is a member of the advisory board of various technical societies and academic committees of different institutes/universities. He is a reviewer of several SCI-indexed journals on high-impact factors. He holds 520 rank in India, in the list of world's scientists, released by AI index.

**Pooja Singh** completed her Ph.D. from the Department of Mathematical Sciences, Indian Institute of Technology (Banaras Hindu University), Varanasi. She has a rich experience of fourteen years in mathematical modeling, stochastic processes, reliability and safety engineering for safety critical systems and worked in many domains including medical; and image processing in nuclear energy. She has published several

research papers in journals. She supervises many Ph.D. students at reputed institutes. She has many reputed publications related to her field of research. She is a reviewer of many reputed journals on high-impact factors. She is a recipient of a publication award from IIT (BHU). She has completed several industrial projects. She is a member of the editorial board of many international journals and the Guest Lead editor of many special issues of international journals. She is a Senior member of IEEE. She is a life member of the Indian Nuclear Society, Department of Atomic Energy, Government of India.

**Ajit K. Verma** is a Professor of Technical Safety and has been associated with the Western Norway University of Applied Sciences in Haugesund, Norway since March 2012. Before that, he worked as a Professor/Senior (HAG) Scale Professor in the Reliability Engineering/Department of Electrical Engineering at IIT Bombay for around 15 years. His research interests include reliability, risk, safety engineering, and computational intelligence applications. He is also a Guest Professor at Lulea University of Technology in Sweden and was an Adjunct at the University of Stavanger. Dr. Verma has been recognized with several awards, including the “Honorary Professor” and “Global Academic Excellence Award” at Amity University in India. He is the Patron and Founding Editor-in-Chief of *IJSA*, a publication by Springer, and also serves as an Editor-in-Chief of *Life Cycle Reliability and Safety Engineering*, another Springer publication. Additionally, he is the Springer Book Series Editor for five series. He has jointly authored/edited several books published by Springer and has over 250 publications in various journals and conferences. He has also supervised/co-supervised 39 Ph.D. theses.

# Abbreviations

AD	Activity Diagram
AERB	Atomic Energy Regulatory Board
ALT	Alternative
AOPN	Aspect Oriented Petri Nets
AOSPN	Aspect Oriented Stochastic Petri Net
AT	Attack Tree
BC	Backup Computer
BFV	Bypass Feedwater Valve Controller
CCSA	Collision Candidate of System Action
CIA	Confidentiality, Integrity, or Availability
CPN	Colored Petri Net
CSRF	Cross-Site Request Forgery
CTMC	Continuous Time Markov Chain
DCS	Distributed Control System
DFWCS	Digital Feedwater Control System
DoS	Denial of Service Attack
ETA	Event Tree Analysis
FMEA	Failure Modes and Effect Analysis
FP	Feed Pump
FPN	Fuzzy Petri Net
FPT	Fault Prevention Tree
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Analysis
HPN	High Petri Net
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MCS	Minimal Cut Set
MFV	Main Feedwater Valve Controller
MSSV	Main Steam Safety Valve
MTBF	Mean Time between Failures



MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NUREG	Nuclear Regulatory Report
ORS	Online Refueling System
PDI	Pressurized Differential Indicator
PHWR	Pressurized Water Reactor
P-invariant	Place Invariant
PLC	Programmable Logic Controller
PN	Petri Net
PPN	Possibilistic Petri Net
PPTCPN	Piping Possibilistic Petri Net
RAG	Resource Allocation Graph
RBD	Reliability Block Diagram
RG	Regulatory Guide
RTS	Real-Time System
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCS	Safety-Critical System
SD	Sequence Diagram
SDLC	Software Development Life Cycle
SG	Steam Generator
SLR	Systematic Literature Review
SPN	Stochastic Petri Net
T-invariant	Transition Petri Net
TOCTOU	Time-Of-Check-To-Time-Of-Use
TPN	Time Petri Net
UML	Unified Modeling System
XSS	Cross-Site Scripting

# List of Figures

Fig. 1.1	Types of fault	8
Fig. 1.2	Error-fault-failure	10
Fig. 1.3	Types of error	11
Fig. 1.4	Means to attain dependability	13
Fig. 2.1	Types of critical systems	19
Fig. 2.2	Structure of SCS [6]	22
Fig. 2.3	Components of safety-critical controller [6]	23
Fig. 2.4	Any event that becomes uncontrolled will have a negative effect on certain assets. Hazard versus risk	25
Fig. 2.5	Accident scenario	26
Fig. 2.6	Applications of safety critical system	28
Fig. 2.7	Safety-critical systems	29
Fig. 2.8	Generic phases of the SCS analysis	35
Fig. 3.1	Cyberincidents	41
Fig. 3.2	Vulnerabilities in information system	43
Fig. 3.3	Vulnerabilities	44
Fig. 3.4	Types of cyberthreat actor	49
Fig. 3.5	Masquerade	52
Fig. 3.6	Message modification	53
Fig. 3.7	Repudiation	53
Fig. 3.8	Reply attack	54
Fig. 3.9	Denial of service	54
Fig. 3.10	Release of message	55
Fig. 3.11	Traffic analysis	56
Fig. 3.12	Types of cyberattacks	57
Fig. 3.13	SCADA architecture	60
Fig. 3.14	Distributed control system	62
Fig. 3.15	Remote telemetry unit	63
Fig. 3.16	Programmable logic controller (PLC)	65
Fig. 3.17	Cybersecurity types/domains	67
Fig. 4.1	Security metrics	84

Fig. 4.2 Confidentiality tools ..... 85

Fig. 4.3 Tools for integrity ..... 87

Fig. 4.4 Tools of availability ..... 88

Fig. 4.5 Key survivability properties ..... 89

Fig. 4.6 Digital signatures ..... 89

Fig. 4.7 Authentication ..... 91

Fig. 4.8 Authentication tools ..... 92

Fig. 4.9 Sample space ..... 97

Fig. 4.10 **a)** Complement of event  $E$ ; **b)** union of events  $E_{v_1}$  and  $E_{v_2}$ ;  
**c)** intersection of events  $E_{v_1}$  and  $E_{v_2}$  **d)** events  $E_{v_1}$  and  $E_{v_2}$   
are mutually exclusive ..... 101

Fig. 5.1 FTA model ..... 110

Fig. 5.2 FTA of DFWCS ..... 112

Fig. 5.3 ETA of DFWCS ..... 116

Fig. 5.4 ETA of the reactor’s radioactive release ..... 117

Fig. 5.5 Block diagram of Markov model ..... 118

Fig. 5.6 Representation of Markov model 1 ..... 118

Fig. 5.7 Representation of Markov model 2 ..... 119

Fig. 5.8 Sample of PN model ..... 122

Fig. 5.9 PN model of DFWCS ..... 123

Fig. 5.10 Timed Petri net ..... 124

Fig. 5.11 Colored Petri net ..... 125

Fig. 5.12 AT for reactor trip due to low SG level ..... 140

Fig. 5.13 An attack tree for energy theft ..... 141

Fig. 5.14 Series structure of RBD ..... 144

Fig. 5.15 Example of an RBD of the sensor/computer/controller  
and actuator devices of DFWCS ..... 144

Fig. 5.16 Example of an RBD for aircraft power system ..... 145

Fig. 5.17 Scenario graph of the DFWCS ..... 147

Fig. 5.18 Scenario graph of the Browns Ferry case ..... 148

Fig. 5.19 Vehicle speed sensor subsystem ..... 150

Fig. 6.1 FTA analysis process ..... 158

Fig. 6.2 FTA for communication faults in electric energy meter ..... 159

Fig. 6.3 Analysis process of ETA ..... 161

Fig. 6.4 Event tree of LOCA ..... 162

Fig. 6.5 Markov model’s analysis process ..... 163

Fig. 6.6 Petri net model’s analysis process ..... 164

Fig. 6.7 PN model of DFWCS ..... 165

Fig. 6.8 Reachability graph ..... 166

Fig. 6.9 State model ..... 169

Fig. 6.10 PN model ..... 171

Fig. 6.11 Reachability graph of modeled system ..... 171

Fig. 6.12 Analysis steps of HAZOP ..... 174

Fig. 6.13 Analysis steps of SWIFT ..... 177

Fig. 6.14 RBD model of DFWCS ..... 182

Fig. 6.15 Analysis steps of FMEA ..... 184  
Fig. 6.16 FMECA analysis process ..... 186  
Fig. 6.17 Analysis steps of scenario graph ..... 192  
Fig. 6.18 Process of FFA ..... 193  
Fig. 6.19 Attack tree ..... 195  
Fig. 6.20 Markov model ..... 198

# List of Tables

Table 2.1	Catastrophic accidents [8] .....	30
Table 3.1	Standards .....	70
Table 3.2	Characteristics of standards .....	71
Table 4.1	Laptops sold number of days .....	102
Table 5.1	Event symbols of FTA .....	113
Table 5.2	States (Markov model's state) description .....	118
Table 5.3	Place and transition description of the PN model (Fig. 5.9) ...	123
Table 5.4	FMEA of the MFV of DFWCS .....	127
Table 5.5	FMEA of refueling machine .....	128
Table 5.6	FMECA example of DFWCS .....	130
Table 5.7	Guidewords .....	132
Table 5.8	HAZOP worksheet for MFV controller .....	134
Table 5.9	SWIFT example (LNG transport by tank truck and DFWCS) .....	139
Table 5.10	FFA for the example of the vehicle velocity sensor .....	149
Table 6.1	Probability statistics .....	160
Table 6.2	Probability coefficient of the basic event .....	161
Table 6.3	LOCA .....	162
Table 6.4	$P_i$ and $T_j$ description of model (Fig. 6.7) .....	165
Table 6.5	Rate of transition (in per sec) .....	171
Table 6.6	HAZOP report .....	176
Table 6.7	Probability of occurrence .....	177
Table 6.8	Guidewords .....	177
Table 6.9	RBD of the DFWCS .....	183
Table 6.10	DFWCS reliability in the first work year .....	184
Table 6.11	FMEA Report .....	185
Table 6.12	FMEA severity score .....	188
Table 6.13	Calculation conditions for $O,S,D$ of possible hazards .....	190
Table 6.14	FMECA report .....	191
Table 6.15	Consequence rating in FFA [13] .....	193
Table 6.16	Description of the AT (Fig. 6.19) nodes .....	195

Table 6.17	SRL classification matrix . . . . .	196
Table 6.18	Assessment result of the security attack risk . . . . .	196
Table 6.19	Security risk level . . . . .	196
Table 6.20	Comparison of analysis techniques . . . . .	202