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

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 ISSN 2522-5170 (electronic)
Asset Analytics
ISBN 978-981-97-4017-8 ISBN 978-981-97-4018-5 (eBook)
https://doi.org/10.1007/978-981-97-4018-5

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 — Raj Kamal Kaur
Mumbai, India — Lalit Kumar Singh
Navi Mumbai, India — Pooja Singh
Haugesund, Norway — 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 scritical 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

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

List of Tables