Springer Series in Reliability Engineering

Series Editor

Professor Hoang Pham
Department of Industrial and Systems Engineering
Rutgers, The State University of New Jersey
96 Frelinghuysen Road
Piscataway, NJ 08854-8018
USA

Other titles in this series

The Universal Generating Function in Reliability Analysis and Optimization
Gregory Levitin

Warranty Management and Product Manufacture
D.N.P. Murthy and Wallace R. Blischke

Maintenance Theory of Reliability
Toshio Nakagawa

System Software Reliability
Hoang Pham

Reliability and Optimal Maintenance
Hongzhou Wang and Hoang Pham

Applied Reliability and Quality
B.S. Dhillon

Shock and Damage Models in Reliability Theory
Toshio Nakagawa

Risk Management
Terje Aven and Jan Erik Vinnem

Satisfying Safety Goals by Probabilistic Risk Assessment
Hiromitsu Kumamoto

Offshore Risk Assessment (2nd Edition)
Jan Erik Vinnem

The Maintenance Management Framework
Adolfo Crespo Márquez

Human Reliability and Error in Transportation Systems
B.S. Dhillon

Complex System Maintenance Handbook
D.N.P. Murthy and Khairy A.H. Kobbacy

Recent Advances in Reliability and Quality in Design
Hoang Pham

Product Reliability
D.N.P. Murthy, Marvin Rausand and Trond Østerås

Mining Equipment Reliability, Maintainability, and Safety
B.S. Dhillon

Advanced Reliability Models and Maintenance Policies
Toshio Nakagawa

Justifying the Dependability of Computer-based Systems
Pierre-Jacques Courtois

Poong Hyun Seong
Editor

Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems

With Additional Contributions by
Poong Hyun Seong
Hyun Gook Kang
Han Seong Son
Jong Gyun Choi
Man Cheol Kim
Jong Hyun Kim
Jae Whan Kim
Seo Ryong Koo
Seung Jun Lee
Jun Su Ha

Springer

Professor Poong Hyun Seong, PhD
Department of Nuclear
and Quantum Engineering
Korea Advanced Institute of Science
and Technology (KAIST)
373-1, Guseong-dong, Yuseong-gu
Daejeon, 305-701
Republic of Korea

ISBN 978-1-84800-383-5 e-ISBN 978-1-84800-384-2

DOI 10.1007/978-1-84800-384-2

Springer Series in Reliability Engineering ISSN 1614-7839

British Library Cataloguing in Publication Data
Reliability and risk issues in large scale safety-critical
digital control systems. - (Springer series in reliability
engineering)
1. Digital control systems 2. Digital control systems -
Reliability
I. Seong, Poong Hyun
629.8'312
ISBN-13: 9781848003835

Library of Congress Control Number: 2008933411

Cover design: deblik, Berlin, Germany

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Preface

Reliability and risk issues for safety-critical digital control systems are associated with hardware, software, human factors, and the integration of these three entities. The book is divided into four parts. Each part, consisting of three chapters, deals with all entities.

Component level digital hardware reliability, existing hardware reliability theories, and related digital hardware reliability issues (Chapter 1), digital system reliability and risk including hardware, software, human factors, and integration (Chapter 2), and countermeasures using cases from nuclear power plants (Chapter 3) are presented in Part I.

Existing software reliability models and associated issues (Chapter 4), software reliability improvement techniques as countermeasures of software reliability modeling (Chapter 5), and a CASE tool called "NuSEE (nuclear software engineering environment)" which was developed at KAIST (Chapter 6) are presented in Part II.

Selected important existing human reliability analysis (HRA) methods including first- and second-generation methods (Chapter 7), human factors considered in designing and evaluating large-scale safety-critical digital control systems (Chapter 8), and a human performance evaluation tool, called "HUPESS (human performance evaluation support system)", which was developed at KAIST as a countermeasure to human-factors-related issues (Chapter 9) are presented in Part III.

The integrated large-scale safety-critical control system, which consists of hardware and software that is usually handled by humans, is presented in Part IV. This book emphasizes the need to consider hardware, software, and human factors, not separately, but in an integrated manner. Instrument failure significantly affecting human operator performance was demonstrated in many cases, including the TMI-2 incidents. These issues are discussed in Chapter 10. An analytical HRA method for safety assessment of the integrated digital control systems including human operators, which is based on Bayes' theorem and information theory, is discussed in Chapter 11. Using this method, it is concluded that human operators are crucial in reliability and risk issues for large-scale safety-critical digital control systems. An operator system which supports human cognitive behavior and actions, "INDESCO (integrated decision support system to aid the cognitive activities of operators)" which was developed at KAIST is discussed in Chapter 12.

This book can be read in different ways. If a reader wants to read only the current issues in any specific entity, he/she can read the first two chapters of either Part I, II, or III, or the first chapter of Part IV. If a reader wants to read only countermeasures developed at KAIST in any specific entity, he/she may read either Chapter 3, 6, or 9, or Chapters 11 and 12.

There are many co-authors of this book. Part I was mainly written by Drs. Jong Gyun CHOI and Hyun Gook KANG from KAERI (Korea Atomic Energy Research Institute). Part II was mainly written by Professor Han Seong SON from Joongbu University and Dr. Seo Ryong KOO from Doosan Heavy Industries and Construction Co., Ltd.. The main writers of Part III are Mr. Jae Whan KIM from KAERI, Dr. Jong Hyun KIM from KHNP (Korea Hydro and Nuclear Power) Co., Ltd., and Dr. Jun Su HA from KAIST. The integration part, Part IV, was mainly written by Drs. Man Cheol KIM and Seung Jun LEE from KAERI.

Last but not least, I would like to thank Mrs. Shirley Sanders and Professor Charles Sanders for their invaluable support for English editing of this entire book. Without their help, this book might have not been published.

Republic of Korea
May 2008

Poong Hyun Seong

Professor
Department of Nuclear
and Quantum Engineering
Korea Advanced Institute
of Science and Technology (KAIST)

Contents

Part II Software-related Issues and Countermeasures

List of Contributors

Poong Hyun Seong
Department of Nuclear and Quantum Engineering,
Korea Advanced Institute of Science and Technology (KAIST)

Hyun Gook Kang
Integrated Safety Assessment Division,
Korea Atomic Energy Research Institute (KAERI)

Han Seong Son
Department of Game Engineering, Joongbu University

Jong Gyun Choi
I&C and Human Factors Division, KAERI

Man Cheol Kim
Integrated Safety Assessment Division, KAERI

Jong Hyun Kim
MMIS Team, Nuclear Engineering and Technology Institute (NETEC),
Korea Hydro and Nuclear Power (KHNP) Co., Ltd.

Jae Whan Kim
Integrated Safety Assessment Division, KAERI

Seo Ryong Koo
Nuclear Power Plant BG, Doosan Heavy Industries and Construction Co., Ltd.

Seung Jun Lee
Integrated Safety Assessment Division, KAERI

Jun Su Ha
Center for Advanced Reactor Research, KAIST

List of Figures

List of Tables