Studies in Systems, Decision and Control

Volume 272

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

The series "Studies in Systems, Decision and Control" (SSDC) covers both new developments and advances, as well as the state of the art, in the various areas of broadly perceived systems, decision making and control–quickly, up to date and with a high quality. The intent is to cover the theory, applications, and perspectives on the state of the art and future developments relevant to systems, decision making, control, complex processes and related areas, as embedded in the fields of engineering, computer science, physics, economics, social and life sciences, as well as the paradigms and methodologies behind them. The series contains monographs, textbooks, lecture notes and edited volumes in systems, decision making and control spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

** Indexing: The books of this series are submitted to ISI, SCOPUS, DBLP, Ulrichs, MathSciNet, Current Mathematical Publications, Mathematical Reviews, Zentralblatt Math: MetaPress and Springerlink.

More information about this series at http://www.springer.com/series/13304

Hans-Dieter Kochs

Dependability of Engineering Systems

A Markov Minimal Cut Approach

Springer

Hans-Dieter Kochs
Lehrstuhl für Informationslogistik
Universität Duisburg-Essen
Duisburg, Germany

ISSN 2198-4182 ISSN 2198-4190 (electronic)
Studies in Systems, Decision and Control
ISBN 978-3-030-38326-8 ISBN 978-3-030-38327-5 (eBook)
https://doi.org/10.1007/978-3-030-38327-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The dependability (defined in IEC 60050-192:2015) of engineering systems is strongly affected by stochastic dependencies (s-dependencies) between their components. Whenever a system crash occurs, it is always considered as a "concatenation of tragic circumstances", but detailed analyses have mostly uncovered that system failures are caused by inadequate system design and s-dependencies between components, often triggered by common cause failures (*CCF*) or, in the worst case, by systematic failures. Also, the increasing interactions between components of complex structured systems as well as preventive and corrective maintenance (repair) strategies can cause s-dependencies and strongly affect system dependability. The recent severe crashes of two airplanes of the type Boing 737 Max in 2018 and the failure of the Galileo satellite navigation system in 2019 underline the increasing importance of designing redundant structures including human interaction for systems with high dependability requirements. Therefore, a challenge is the accurate modeling and calculation of the dependability of system structures in order to identify weaknesses in the system design and to assess the impact of s-dependency on system dependability. A particular interest in this book focuses on the impact of s-dependency on system-relevant redundant structures.

Dependability analysis method. The *Markov minimal cut* (*MMC*) approach combined with the *probable Markov path* (*pMp*) approach is a powerful method for the evaluation of the dependability of large and complex engineering systems including s-dependent components. A *MMC* is a minimal cut (*MC*) which is modeled as a Markov process. The main task in the development process of *MMC* is to create Markov process models (Markov models), which are compatible to the *MC*. The mathematical basics and the procedure to create these models are described in (Kochs 2017).

What is new? The newly introduced systematics in the following chapters gives an in-depth understanding of *precise* and *approximate MMC* modeling and calculation techniques of engineering systems, which has not been addressed in previous works. The in-depth analysis demonstrates that it is only possible to *precisely* model and calculate the dependability of systems including s-dependent components with the knowledge of their (total) universe spaces, represented here by

Markov spaces. They provide the basis for developing and verifying a*pproximated MMC* models for engineering systems. Missing universe spaces can be a severe problem for dependability analyses (apart from the lack of data and data uncertainty). However, with the assumption of using realistic parameter values, *approximated MMC* models of systems can be developed without consideration of the total Markov spaces. Many examples of redundant structures show clearly the universal application of *MMC* modeling and calculation techniques with emphasis on model accuracy.

Objective of this book. The book persues the following aims with focus on reliability, availability, and safety: (1) Determination of the minimal cuts (*MC*) of systems; (2) *New: Precise* modeling of the Markov minimal cuts (*MMC*), based on the equivalence between logical networks and Markov space models including s-dependencies; (3) Development of *approximated MMC* models and analytical calculation of their indices using the probable Markov path (*pMp*) approach; (4) Integration of *MMC* models into the framework of Fig. 1.2 and calculation of the system indices; (5) Application of the *MMC* approach to several examples, which represent basic redundant structures of engineering systems; (6) Estimation of the impact of s-dependencies on systems using the stochastic dependency impact (*sDI*) factor; (7) *New:* Comparison between *exact* and *approximate* results. Points 1 to 4 represent the main steps of the *MMC* approach. Special emphasis is placed on Points 1 and 7 in combination with Points 2, 3, and 4, which is new. With the mathematical steps, described and applied to several examples throughout this text, interested system developers and users can perform dependability analyses themselves. All examples are structured in precisely the same way.

Prerequisite. Mathematical interest, basic knowledge of dependability and Boolean algebra, probability theory, and theory of stochastic processes.

Expression of thanks. I particularly would like to thank Prof. Dr. K. Echtle from the university of Duisburg-Essen and the community of the Fault Tolerant Discussion Panel (Diskussionskreis Fehlertoleranz, FG-FERS) as well as Dr. J. Petersen for their substantial contributions and discussions. Furthermore, I would like to cordially thank Dr. J. Nachtkamp for his profound comments and remarks. He is one of the former initiators of the probable Markov path approach and its integration into the minimal cut approach for power systems and substations at the Institute of Power Systems and Power Economics (IAEW) at the RWTH Aachen. I am very grateful to Ms. S. Heidtmann for many remarks and proofreading of the manuscript.

Finally, but by no means least, I would like to particularly highlight and cordially thank my wife Anne for her support during the creation of this book.

Special thanks are also due to the Springer staff, especially Dr. J.-P. Schmidt, Prof. Dr. J. Kacprzyk, and Ms. P. Jantzen as well as the Springer production team for their editorial support.

Duisburg, Germany Hans-Dieter Kochs
Nov 2019

Contents

About the Author

Hans-Dieter Kochs obtained a Diploma degree in Electrical Engineering (1972) and a Dr.-Ing. degree (1976) from the Technical University (RWTH) Aachen, Germany (scholarship of the Cusanuswerk). From 1972 to 1979, he was a research assistant at the Institute of Power Systems and Power Economics (IAEW, headed by Prof. Dr. K. W. Edwin) at the RWTH Aachen. From 1979 to 1991, he held leading positions in industry (AEG/Daimler Frankfurt, FAG Kugelfischer Erlangen, and ESWE Wiesbaden, Germany). From 1991 to 2010, he was head of the Chair of Computer Engineering and Information Logistics at the Faculty of Engineering of the University of Duisburg-Essen, Germany. From 1972 to the present day, the author has been engaged in numerous scientific and industrial dependability analyses and studies. He is a proven expert for reviewing scientific and industrial analyses and studies.

Symbols and Abbreviations

No distinction is made between singular and plural notation of the abbreviations. For example, *DBD*, *CCF*, *MC*, *MMC*, and *pMp* indicate the singular as well as the plural form.

$a_{j,k}$	Constant transition rate from $Z_j \rightarrow Z_k$
AND	Logical AND (conjunction, $\wedge$)
$CCF,\ CCF_{i,k}$	Common cause failure, impact of component i on k
$c_{i,k}$	Probability of $CCF_{i,k},\ 0 \leq c_{i,k} \leq 1$
D, D_i, D_S	Down state due to failure, of component i, of system S
DBD	Dependability block diagram $\equiv$ logical diagram or logical network which represents the up state mode (similar to a reliability block diagram *RBD*, but used in a more general context concerning the integration of the *MMC* models)
Δ	Deviation, model inaccuracy (quantified in the tables)
DFG	German Research Foundation (Deutsche Forschungsgemeinschaft)
$Fr(Z)$	Frequency of state Z (steady state)
MC	Minimal cut
$\overline{MC}$	$\equiv \neg MC$ (up state mode in relation to *MC*)
MMC	Markov minimal cut
$\overline{MMC}$	$\equiv \neg MMC$ (up state mode in relation to *MMC*)
MTTSF	Mean operating time to system failure
n, n_{MMC}, n_Z	Number, number of *MMC,* number of Z
$\Omega, \Omega_i, \Omega_S$	Universe space, of component i, of system $S,\ Pr(\Omega_{...}) = 1$ ($\Omega_{...}$ represented by Markov spaces)
OR	Logical OR (disjunction, $\vee$)
pMp	Probable Markov path
$Pr(Z), Pr(Z_{ind}), Pr(Z_{dep})$	Probability of state Z (steady state), of s-*ind*ependent Z, of s-*dep*endent Z

RBD	Reliability block diagram (replaced by *DBD*)
roon	*r*-out-of-*n*, $1 \leq r \leq n,\ n \geq 1$
S	Index for system
$sDI(\ldots)$	s-Dependency impact of *MMC* and D_S
$sDI(\ldots)$-factor	$= Pr(\ldots_{dep})/Pr(\ldots_{ind})$
SFB	German Collaborative Research Centre of the DFG (Sonderforschungsbereich 291 der DFG)
$Ti(Z)$	Mean time (duration) of state *Z* (steady state)
U, U_i, U_S	Up state (operating state), of component *i*, of system *S*
x_C	Limit value for *c*, depending on the acceptable Δ
X, *Z*	Markov states
λ, μ	Constant failure rate, constant restoration ($\equiv$ repair) rate, $\lambda < \mu$

List of Figures

List of Tables