

Berichte aus der Automatisierungstechnik

Konstantin Machleidt

**Preventive maintenance of Safety-related Systems –
modeling, analysis, and optimization**

Präventive Instandhaltung sicherheitsbezogener Systeme –
Modellierung, Analyse und Optimierung

D 386 (Diss. Technische Universität Kaiserslautern)

Shaker Verlag
Aachen 2016

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Zugl.: Kaiserslautern, TU, Diss., 2015

Copyright Shaker Verlag 2016

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 978-3-8440-4151-4

ISSN 0945-4659

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen

Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9

Internet: www.shaker.de • e-mail: info@shaker.de

Preventive maintenance of Safety-related Systems – modeling, analysis, and optimization

Präventive Instandhaltung sicherheitsbezogener Systeme – Modellierung,
Analyse und Optimierung

Vom Fachbereich Elektrotechnik und Informationstechnik
der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Ingenieurwissenschaften (Dr.-Ing.)
genehmigte Dissertation

von
Dipl.-Ing. Konstantin Machleidt
geb. in Nowosibirsk

D 386

Datum der mündlichen Prüfung:	30.10.2015
Dekan des Fachbereichs:	Prof. Dr.-Ing. Hans D. Schotten
Promotionskommission	
Vorsitzender:	Prof. Dr. techn. Gerhard Fohler Technische Universität Kaiserslautern
Berichterstattende:	Prof. Dr.-Ing. habil. Ping Zhang Technische Universität Kaiserslautern
	Prof. Dr.-Ing. Frank Schiller Beckhoff Automation GmbH & Co. KG und East China University of Science and Technology

Abstract: Safety-related Systems (SRS) protect from the unacceptable risk resulting from failures of technical systems. The average probability of dangerous failure on demand (PFD) of these SRS in low demand mode is limited by standards. Probabilistic models are applied to determine the average PFD and verify the specified limits. In this thesis an effective framework for probabilistic modeling of complex SRS is provided. This framework enables to compute the average, instantaneous, and maximum PFD. In SRS, preventive maintenance (PM) is essential to achieve an average PFD in compliance with specified limits. PM intends to reveal dangerous undetected failures and provides repair if necessary. The introduced framework pays special attention to the precise and detailed modeling of PM. Multiple so far neglected degrees of freedom of the PM are considered, such as two types of elementwise PM at arbitrarily variable times. As shown by analyses, these degrees of freedom have a significant impact on the average, instantaneous, and maximum PFD. The PM is optimized to improve the average or maximum PFD or both. A well-known heuristic nonlinear optimization method (Nelder-Mead method) is applied to minimize the average or maximum PFD or a weighted trade-off. A significant improvement of the objectives and an improved protection are achieved. These improvements are achieved via the available degrees of freedom of the PM and without additional effort. Moreover, a set of rules is presented to decide for a given SRS if significant improvements will be achieved by optimization of the PM. These rules are based on the well-known characteristics of the SRS, e.g. redundancy or no redundancy, complete or incomplete coverage of PM. The presented rules aim to support the decision whether the optimization is advantageous for a given SRS and if it should be applied or not.

Zusammenfassung: Sicherheitsbezogene Systeme (SRS) schützen vor unverhältnismäßigen Gefährdungen, die durch Ausfälle technischer Einrichtungen verursacht werden. Die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung (PFD) für die SRS mit niedriger Anforderungsart wird durch Normen begrenzt. Um die mittlere PFD zu ermitteln und die durch Normen vorgeschriebenen Grenzwerte zu verifizieren, werden probabilistische Modelle verwendet. In dieser Dissertation wird eine neue Methode zur probabilistischen Modellierung komplexer SRS entwickelt, mit der die Kenngrößen mittlere, instantane und maximale PFD ermittelt werden können. Für SRS ist die präventive Instandhaltung (PM) unentbehrlich, damit die mittlere PFD die vorgeschriebenen Grenzwerte nicht überschreitet. Durch PM werden die gefahrbringenden unerkannten Ausfälle aufgedeckt und falls erforderlich repariert. Bei der entwickelten Methode wird ein besonderes Augenmerk auf die präzise und detaillierte Modellierung der PM gelegt. Es werden mehrere bisher vernachlässigte Freiheitsgrade der PM berücksichtigt, wie z.B. für jedes Element zwei Typen der PM, jeweils zu beliebigen variablen Zeiten. Wie in Analysen gezeigt wird, haben diese Freiheitsgrade einen signifikanten Einfluss auf die Kenngrößen. Um eine Verbesserung der mittleren oder maximalen PFD oder von beiden

zu erzielen, wird die PM optimiert. Mittels eines Verfahrens der heuristischen nichtlinearen Optimierung (Nelder-Mead-Verfahren) werden die mittlere oder maximale PFD oder eine gewichtete zusammengesetzte Zielfunktion minimiert. Es werden signifikante Verbesserungen der Optimierungsziele und ein besserer Schutz vor Gefährdungen erreicht. Diese Verbesserungen werden mittels verfügbarer Freiheitsgrade der PM erzielt und erfordern keinen Mehraufwand. Zusätzlich werden Regeln bereitgestellt, um abzuschätzen ob für ein SRS signifikante Verbesserungen durch die Optimierung erzielt werden können. Diese Regeln basieren auf den bekannten Merkmalen des SRS, wie z.B. Redundanz oder keine Redundanz, vollständige oder unvollständige Abdeckung der PM. Damit lässt es sich abschätzen, ob der Einsatz der beschriebenen Optimierungsmethoden für ein SRS vorteilhaft sein kann.

Acknowledgments

The work that resulted in this book could not have been accomplished without several persons' assistance, support, and encouragement.

First of all, I would like to thank my doctoral adviser, Professor **LOTHAR LITZ**, for the opportunity to research and work at his institute. I am deeply grateful for his encouragement, the trust he placed in my work, and the intellectual freedom he has given to me in these years. His guidance and invaluable advice were of great importance to complete this work. The research standards he has propagated were worthy of imitation and influenced me strongly. Tragically, Professor **LOTHAR LITZ** suddenly passed away this August. This book is dedicated to him.

My sincere thanks go to the members of the evaluation board: Professor **PING ZHANG**, Technische Universität Kaiserslautern; Professor **FRANK SCHILLER**, Beckhoff Automation GmbH & Co. KG and East China University of Science and Technology; and the chairman Professor **GERHARD FOHLER**, Technische Universität Kaiserslautern.

During my work as a research associate for the Institute of Automatic Control at the Technische Universität Kaiserslautern I had the privilege to be part of a great team. I am grateful to all my colleagues for the numerous rich and important discussions about research and other interesting topics. Thank you for your friendship, support, and humor. I deeply appreciate the time we had spent together at the institute, on our joint trips, and during the numerous activities apart from work. Many thanks to **STEFAN SCHNEIDER**, **THOMAS GABRIEL**, **THORSTEN RODNER**, **ANNA NEHRING**, **THOMAS LEIFELD**, **ANDRÉ TELES-CARVALHO**, and **ANDREAS HAUPT** for proofreading of the manuscript and hinting at a considerable number of flaws I have eliminated with your help.

During my work for the Institute of Automatic Control, I was part of several industrial projects with the companies **KROHNE Messtechnik GmbH**, **Bayer TechnologyServices GmbH**, and **BASF SE**. I would like to warmly thank all the people who contributed to successfully complete these projects.

My sincere thanks go to **THOMAS GABRIEL**, **DANIEL DÜPONT**, and **ANDREAS HILDEBRANDT** for the numerous interesting and inspiring discussions on the topic of functional safety. I would like to thank **CHRISTOPH JÖTTEN** for his always helpful and inspiring advice. Moreover, I would like to thank my friends and relatives for the support and encouragement they gave me during these years.

Finally, and not the least, I give the heartiest gratitude to LUCIA and to my parents for their love, patience, encouragement, and help.

Kaiserslautern, December 2015

KONSTANTIN MACHLEIDT

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Background and state of the art	3
1.3	Novel contributions	15
1.4	Organization	16
2	Safety-related Systems (SRSs)	19
2.1	Preliminaries	19
2.2	Failure	21
2.2.1	Definition	21
2.2.2	Random hardware failure vs. systematic failure	21
2.2.3	Failure modes	24
2.3	Maintenance	28
2.3.1	Preliminaries	28
2.3.2	Corrective maintenance	29
2.3.3	Preventive maintenance	30
2.4	Figures of merit	32
2.4.1	Preliminaries	32
2.4.2	Reliability and frequency of a dangerous failure (PFH)	32
2.4.3	Availability and probability of dangerous failure on demand (PFD)	33
3	Modeling via Stochastic and Deterministic Timed Automata (SDTAs)	37
3.1	Preliminaries	37
3.2	SDTA definition	38
3.2.1	Preliminaries	38
3.2.2	Deterministic timed events	38
3.2.3	Exponential stochastic timed events	39
3.2.4	Model of an SRS	40
3.3	Procedure to model SRS with multiple elements	47
3.3.1	Preliminaries	47
3.3.2	The SRS element	47

3.3.3	Parallel composition	50
3.3.4	Dependent SRS elements	51
3.3.5	SRS elements with common-cause failures	52
3.4	Discussion on SDTAs	54
4	Probabilistic evaluation of the SDTAs via Multi-phase Continuous-time Markov Chains (MP-CMCs)	57
4.1	Preliminaries	57
4.2	MP-CMC definition	57
4.3	SDTA transformation into MP-CMC	61
4.4	Preventive maintenance (PM) plans and strategies	65
4.4.1	Preliminaries	65
4.4.2	Definition of PM plan	65
4.4.3	Restrictions on PM plans	65
4.4.4	Definition of PM strategies	68
5	Model analysis and validation	71
5.1	Preliminaries	71
5.2	Analyzed models	71
5.2.1	Preliminaries	71
5.2.2	One element model	73
5.2.3	Three element model	75
5.2.4	Results	76
5.3	Validation	78
5.3.1	Preliminaries	78
5.3.2	Model of Torres-Echeverría et al.	78
5.3.3	Model of Brissaud et al.	79
5.3.4	Model of IEC 61508	80
5.3.5	Results	80
5.4	Sensitivity analysis	86
5.4.1	Preliminaries	86
5.4.2	Theoretical framework	86
5.4.3	Results	88
6	Optimization of preventive maintenance plans	93
6.1	Preliminaries	93
6.2	Optimization problems	93
6.3	Optimization algorithm	94
6.3.1	Preliminaries	94
6.3.2	Nelder-Mead method	95

6.4	Heuristic approach to minimize the maximum PFD	98
6.5	Results	100
6.5.1	Preliminaries	100
6.5.2	Models without redundancy	102
6.5.3	Models with redundancy	106
6.5.4	Models with redundancy and common-cause failures	110
6.6	General conclusions	113
7	Summaries	117
7.1	Summary in English	117
7.2	Outlook	118
7.3	Extended summary in German – Kurzfassung in deutscher Sprache	119
A	Model of SRS element with reduced number of states	123
B	State classification of selected <i>MooN</i> element structures	127
C	Models of selected dependent SRS elements	129
D	Nomenclature	133
	Bibliography	141
	About the author	145