Dependable Computing and Fault-Tolerant Systems

Edited by

A. Avižienis, H. Kopetz, J. C. Laprie

Volume 2

U. Voges (ed.)

*Software Diversity
in Computerized
Control Systems*

Springer-Verlag Wien New York

Dipl.-Math. Udo Voges, Kernforschungszentrum Karlsruhe GmbH,
Karlsruhe, Federal Republic of Germany

With 41 Figures

This work is subject to copyright.

All rights are reserved,
whether the whole or part of the material is concerned,
specifically those of translation, reprinting, re-use of illustrations,
broadcasting, reproduction by photocopying machine or similar means,
and storage in data banks.

© 1988 by Springer-Verlag/Wien

Softcover reprint of the hardcover 1st edition 1988

Library of Congress Cataloging-in-Publication Data

Software diversity in computerized control systems.

(Dependable computing and fault-tolerant systems ;
vol. 2)

Contents: Introduction / U. Voges — Railway
applications / G. Haglin — Nuclear applications /
U. Voges, P. Bishop — [etc.]

1. Fault-tolerant computing. 2. Computer software—
Reliability. 3. Automatic control—Data processing.
I. Voges, Udo, 1946— . II. Series.

QA76.9.F38S65 1988 005 87-32367

ISBN-13:978-3-7091-8934-4 (U.S.)

ISSN 0932-5581

ISBN-13:978-3-7091-8934-4 e-ISBN-13:978-3-7091-8932-0

DOI: 10.1007/978-3-7091-8932-0

Preface

Software Diversity is one of the fault-tolerance means to achieve dependable systems.

In this volume, some experimental systems as well as real-life applications of software diversity are presented. The history, the current state-of-the-art and future perspectives are given.

Although this technique is used quite successfully in industrial applications, further research is necessary to solve some open questions. We hope to report on new results and applications in another volume of this series within some years.

Acknowledgements

The idea of the workshop was put forward by the chairpersons of IFIP WG 10.4, J.-C. Laprie, J. F. Meyer and Y. Tohma, in January 1986, and the editor of this volume was asked to organize the workshop.

This volume was edited with the assistance of the editors of the series, A. Avižienis, H. Kopetz and J.-C. Laprie, who also had the function of reviewers.

Karlsruhe, October 1987

U. Voges, Editor

Table of Contents

1. Introduction	1
<i>U. Voges</i>	
2. Railway Applications	7
ERICSSON Safety System for Railway Control	11
<i>G. Hagelin</i>	
3. Nuclear Applications	23
Use of Diversity in Experimental Reactor Safety Systems	29
<i>U. Voges</i>	
The PODS Diversity Experiment	51
<i>P. G. Bishop</i>	
4. Flight Applications	85
AIRBUS and ATR System Architecture and Specification	95
<i>P. Traverse</i>	
5. University Research	105
Tolerating Software Design Faults in a Command and Control System	109
<i>T. Anderson, P. A. Barrett, D. N. Halliwell, M. R. Moulding</i>	
DEDIX 87 – A Supervisory System for Design Diversity Experiments at UCLA	129
<i>A. Avižienis, M. R. T. Lyu, W. Schütz, K.-S. Tso, U. Voges</i>	
6. Modelling Issues	169
Reliability Modelling for Fault-Tolerant Software Report on a Workshop Held in Badgastein, Austria, July 1986	173
<i>B. Littlewood, T. Anderson</i>	
7. Conclusion	183
<i>U. Voges</i>	
8. Annotated Bibliography	189
<i>U. Voges</i>	