Advances in Intelligent Systems and Computing 987

Wojciech Zamojski
Jacek Mazurkiewicz
Jarosław Sugier
Tomasz Walkowiak
Janusz Kacprzyk *Editors*

# Engineering in Dependability of Computer Systems and Networks

## Proceedings of the Fourteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, July 1–5, 2019, Brunów, Poland

Springer

# Advances in Intelligent Systems and Computing

Volume 987

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing such as: computational intelligence, soft computing including neural networks, fuzzy systems, evolutionary computing and the fusion of these paradigms, social intelligence, ambient intelligence, computational neuroscience, artificial life, virtual worlds and society, cognitive science and systems, Perception and Vision, DNA and immune based systems, self-organizing and adaptive systems, e-Learning and teaching, human-centered and human-centric computing, recommender systems, intelligent control, robotics and mechatronics including human-machine teaming, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, knowledge management, intelligent agents, intelligent decision making and support, intelligent network security, trust management, interactive entertainment, Web intelligence and multimedia.

The publications within "Advances in Intelligent Systems and Computing" are primarily proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

**** Indexing: The books of this series are submitted to ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springerlink ****

More information about this series at http://www.springer.com/series/11156

Wojciech Zamojski · Jacek Mazurkiewicz ·
Jarosław Sugier · Tomasz Walkowiak ·
Janusz Kacprzyk
Editors

# Engineering in Dependability of Computer Systems and Networks

Proceedings of the Fourteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, July 1–5, 2019, Brunów, Poland

Springer

*Editors*
Wojciech Zamojski
Wrocław University of Science
and Technology
Wroclaw, Poland

Jacek Mazurkiewicz
Wrocław University of Science
and Technology
Wroclaw, Poland

Jarosław Sugier
Wrocław University of Science
and Technology
Wroclaw, Poland

Tomasz Walkowiak
Wrocław University of Science
and Technology
Wroclaw, Poland

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

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-030-19500-7 ISBN 978-3-030-19501-4 (eBook)
https://doi.org/10.1007/978-3-030-19501-4



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

# Contents

# Modelling and Safety Assessment of Programmable Platform Based Information and Control Systems Considering Hidden Physical and Design Faults

Vyacheslav Kharchenko[1,2(✉)], Yuriy Ponochovnyi[3], Anton Andrashov[2], Eugene Brezhniev[1,2], and Eugene Bulba[1,2]

[1] National Aerospace University KhAI, Kharkiv, Ukraine
V.Kharchenko@csn.khai.edu, e.brezhnev@csis.org.ua, evhenb@gmail.com
[2] Research and Production Company Radiy, Kropyvnytskyi, Ukraine
a.andrashov@radiy.com
[3] Poltava State Agrarian Academy, Poltava, Ukraine
yuriy.ponch@gmail.com

**Abstract.** The information and control system (I&CS) of Nuclear Power Plant (NPP) is considered as a set of three independent hardware channels including on-line testing system. NPP I&C system's design on programmable platforms is rigidly tied to the V-model of the life cycle. Functional safety and availability during its life cycle are assessed using Markov models. Markov models are used to assess availability function and proof test period. The basic single-fragment model MICS01 contains an absorbing state in case of hidden faults and allows to evaluate risks of "hidden" unavailability. The MICS02 model simulates "migration" of states with undetected failures into states with detected faults. The results of Markov modeling (models MICS01 and MICS02) are compared to evaluate proof test period taking into account requirements for SIL3 level and limiting values of hidden fault probabilities.

**Keywords:** Functional safety modeling · Information and control system · Availability functions · Undetected failure

## 1 Introduction

Nuclear Power Plant (NPP) information and control systems (I&CSs) such as reactor trip systems are safety critical systems. Very stringent requirements have been developed to such systems characteristics and life cycle processes. During the development cycle, it is possible to change the architecture of the NPP I&CS project, correct the parameters of its elements, program code and other changes. This affects the final characteristics of the system (quality, reliability, availability, safety, etc.).

The software architecture is modified on functions changing or on the detected software faults elimination. This affects code characteristics and failures and recovery


W. Zamojski et al. (Eds.): DepCoS-RELCOMEX 2019, AISC 987, pp. 264–273, 2020.
https://doi.org/10.1007/978-3-030-19501-4_26

flow parameters. In papers [1–3], the mathematical apparatus of Markov and semi-Markov processes was used to study systems with variable indicators. In [4], a systematic approach to the construction of multi-fragment models was considered, which allows to structure complex systems models development. NPP I&CS design on programmable platforms such as RadICS [5] is rigidly tied to the V-model of the life cycle. During the development, verification and validation phases of the project, the results are recorded at intermediate stages. During the execution of the stage, it is possible to change both the system architecture and its parameters. Therefore, the primary developed safety assessment models need to be adjusted for changes and linked to the stages of the V model.

I&CS design of one of the NPP emergency protection system subsystems, previously considered in [5, 6], is investigated in this paper. Block diagram of the I&CS is shown in Fig. 1. It's one-version I&CS which implements logic of voting "2 out of 3". It includes three independent channels basing on programmable (FPGA) modules of the platform, in particular digital and analog input and output modules, logic module. Each channel is checked by the on-line testing systems for the dangerous failures presence. The hardware channels use the similar software (VHDL). If VHDL design faults occur it is equivalent to a common cause failure (CCF). To minimize CCF risk diversity approach (hardware-software components and process version redundancy) is applied [7, 8].

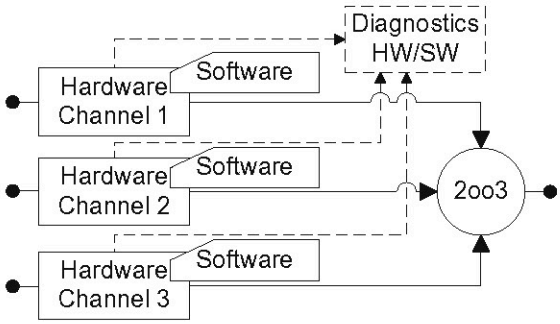


**Fig. 1.** I&CS reliability structural diagram [2].

Control system is characterized by the parameter of on-line test diagnostics coverage (DC). In the designed system, there are distinctions between the diagnostics of the hardware and software with the parameters $DC_{HW}$ and $DC_{SW}$. Control is carried out continuously and the detected failures are eliminated immediately after detection.

The class of I&CS on programmable platforms RadICS [5, 8], which are used in NPP reactors emergency protection systems, is studied in this paper. Emergency protection systems belong to the group of complex objects, which are provided with regular proof tests. These tests are performed according to the regulations and should be treated as a separate process.

# Author Index




W. Zamojski et al. (Eds.): DepCoS-RELCOMEX 2019, AISC 987, pp. 553–554, 2020.
https://doi.org/10.1007/978-3-030-19501-4