Victor Castano · Igor Schagaev

Resilient Computer System Design

Springer

Victor Castano · Igor Schagaev

Resilient Computer System Design

Springer

Resilient Computer System Design

Victor Castano • Igor Schagaev

Resilient Computer System Design

Springer

Victor Castano
IT-ACS Ltd
Stevenage, UK

Igor Schagaev
IT-ACS Ltd and London Metropolitan University
Stevenage, UK

ISBN 978-3-319-15068-0 ISBN 978-3-319-15069-7 (eBook)
DOI 10.1007/978-3-319-15069-7

Library of Congress Control Number: 2015931811

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

New areas of ICT applications require complete redesign of computer systems to address challenges of extreme reliability, high performance and power efficiency. Up to now there are no consistent concepts, theories and texts, enabling us to design systems with mentioned requirements. Requirements themselves became processes and evolve along life cycle of the systems and applications. All these force us to start all over again, leaving past and sentimental values behind, making new computer systems and software that match mentioned requirements and new applications.

Our 35 years of experience consolidates: design of airborne computers and black boxes; parallel computers for submarines, helicopters and satellites. Our intensive research work in academies and higher education institutions included analysis of performance, reliability and design of computer systems. Both regretfully have proved at various levels that existing computer system and system software solutions lack efficiency, rigorousness or balance in design. An absence of a consistent book explaining how to analyse, design and develop new computer systems has been surprisingly revealed. That is why we attempt to introduce—as a first draft—a theory of resilient and evolving systems, as good as we see it today. We introduce rigorous concepts of system design with reconfigurability used when necessary for toleration of faults. Our concepts of redundancy have been theoretically justified and analysed. Redundancy of system we discuss taking into account technological aspects, including thermal barrier and reliability. We propose a new design of system and system software and describe hardware prototypes—to demonstrate feasibility of them. Simulations and trial runs are presented and explained as well.

This book at first was written for ourselves—for everyday work in safety-critical systems design. As it is ICT market and research in this domain are greatly segmented. Thus we had to create our own "meeting point" for all above-mentioned "customers" and addressing new properties of computer systems.

To "start all over again" researchers, engineers, users and even politicians should be ready to understand what future applications of ICT require, what kind of

drawback of technologies we are facing, what are the limitations and how to find the most efficient structural solutions, accompanied by careful use of math methods.

This book is the first consistent work on our paradigm of evolving computers; it includes methods of analysis and synthesis of ICT with new properties such as evolving functioning, performance, reliability and energy-wise solutions. We also discuss abilities of system to match changing requirements and internal faults of hardware schemes, technological advances and drawbacks.

Initially this book did serve us an essential working material in terms of "all you need to know to design and analyze new generation of computer systems" addressing in non-mutually exclusive way reliability, fault tolerance, performance, resilience and properties of electronics, introducing supportive models and key hardware designs: processors, memories and interfaces. We were thinking about the following market our new system that developed, accordingly proposed approach: safety-critical, autonomous, real time, military, banking and wearable health care systems. Presented hardware prototype demonstrates at the order of magnitude higher efficiency in comparison with existing systems.

Who is our reader and why? Research community will get consistent area of further theoretical developments; Industries of hardware and system software designs, manufacturing and exploitation will get pathways to make performance, reliability and energy-smart systems with consistency, enabling unification of market of consumer electronics, safety-critical, embedded, autonomous and autonomous systems; Consumers will get much higher efficiency (and value for money) from their systems (if, of course devices and systems will be designed according to the principles proposed in the book).

This book provides also several personal benefits for the reader:

- Analysis of existing systems given in essence, showing how "classic" solutions stand and work.
- Existing technological drawbacks are clarified and presented consistently, with proposed solutions that "best fit the requirement" of new computer system.
- Description of a process of introduction of new properties as a framework required from next generation of computer system enabling a reader to make consistent analysis of—we stress—all possible system design solutions.
- Demonstrated and described prototype of evolving reconfigurable architecture might be attractive for students as they through the book will discover that computers might be designed much simpler, power efficient and at an order of magnitude more reliable.
- A prototype of the system and simulator will help for future engineers of embedded systems.
- Students and analysts will discover that the market dominance of the general computing systems has been now limited by appeared embedded systems with billions of units manufactured every year. Note that embedded systems appear in contexts where continuous operation is of utmost importance and failure can be profound.

– Any reader will be able to use trail simulator and start programming new architecture.

Nowadays radiation is a serious threat to the reliable operation of safety-critical systems. Fault avoidance techniques, such as radiation hardening, have been commonly used in space applications. However, hardened components are expensive, lag behind commercial components in performance and do not provide 100 % fault elimination. Without supportive structural solutions to provide fault tolerance, hardware faults become system errors at the application or system level, which in turn can result in catastrophic failures.

In this direction, we present known concepts of fault tolerance and dependability and extend them by our own concept of resilience and generalisation of fault tolerance. We propose to consider fault tolerance and resilience as *processes*, instead of properties. We analyse the physics of radiation-induced faults, the damage mechanisms of particles and the error as a consequence.

We propose new approach to hardware and system software design combining efficiently reliability, performance and power consumption.

Finally, to demonstrate how new properties of the computer system will be implemented, a new conceptual system element called a *syndrome* was introduced, described and its application for performance, reliability and energy-smart operations of hardware explained. Implemented by hardware and supported by system software *syndrome* serves as a core of a resilience of architecture enabling system (through software and hardware) be adaptable to various and modifiable functional requirements, different internal conditions and environmental impacts. We implemented a software simulator and disassembler and introduced a testing framework in combination with our evolving reconfigurable architecture assembler and commercial hardware simulators.

Stevenage, UK

Victor Castano
Igor Schagaev

Contents

Abbreviations

ARQ	Automatic repeat quest
ASIC	Application-specific integrated circuit
ASW	Application software
ATPG	Test pattern generation tools
BCH	Bose Chaudhuri hocquenghem
BEC	Backward error correction
BICMOS	Bipolar complementary metal oxide semiconductor
BIST	Built in self-test
BPSG	Boron phosphor silicate glass
CCD	Charged couples device
CED	Concurrent error detection
CM	Corrective maintenance
CMF	Common mode failure
CMOS	Complementary metal oxide semiconductor
COTS	Commercial off the shelf
CSP	Cold standby spare
CUT	Circuit under test
DDD	Displacement damage dose
DEC/TED	Double bit error correction and triple bit error detecting
DFT	Design for testability
DMR	Dual modular redundancy
DRAM	Dynamic random access memory
DRE	Detected recoverable error
DUE	Detected unrecoverable error
DUT	Device under test
DW	Data word
ECC	Error correcting codes
EDAC	Error detection and correction codes
EDC	Error detecting codes
EEPROM	Electrically erasable programmable read only memory