João Alfredo P. de Magalhães

Recovery Oriented Software

TESE DE DOUTORADO

DEPARTAMENTO DE INFORMÁTICA

Postgraduate Program in Informatics

Rio de Janeiro

September 2009

Pontifícia Universidade Católica
do Rio de Janeiro

João Alfredo P. de Magalhães

Recovery Oriented Software

TESE DE DOUTORADO

Thesis presented to the Postgraduate Program in Informatics of the Departamento de Informática, PUC-Rio, as partial fulfillment of the requirements for the degree of Doutor em Informática.

Advisor: Arndt von Staa

Rio de Janeiro

September 2009

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

João Alfredo Pinto de Magalhães

Recovery Oriented Software

Thesis presented to the Postgraduate Program in Informatics, of the Departamento de Informática do Centro Técnico Científico da PUC-Rio, as partial fulfillment of the requirements for the degree of Doutor

Prof. Arndt von Staa
Advisor
Departamento de Informática – PUC-Rio

Profa. Simone Diniz Junqueira Barbosa
Departamento de Informática – PUC-Rio

Prof. Alessandro Fabrício Garcia
Departamento de Informática – PUC-Rio

Prof. Ricardo Choren Noya
Instituto Militar de Engenharia – IME

Profa. Cláudia Maria Lima Werner
Universidade Federal do Rio de Janeiro – UFRJ

Prof. José Eugenio Leal
Coordinator of the Centro Técnico Científico da PUC-Rio

Rio de Janeiro, 03/09/2009

João Alfredo P. de Magalhães

Graduated in Science Computing Engineering from Pontifícia Universidade Católica do Rio de Janeiro (2000, Brazil, Rio de Janeiro), he obtained the degree of Mestre em Informática also from Pontifícia Universidade Católica do Rio de Janeiro (2002, Brazil, Rio de Janeiro).

Bibliographic data

Magalhães, João Alfredo P. de

Recovery oriented software / João Alfredo P. de Magalhães ; advisor: Arndt Von Staa. – 2009.
104 f. : il. ; 30 cm

Tese (Doutorado em Informática)–Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2009.
Inclui bibliografia

1. Informática – Teses. 2. Engenharia de software. 3. Software depurável. 4. Fidedignidade. 5. Corretude por construção. I. Staa, Arndt von. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

CDD: 004

To my parents, Alfredo and Mariza.

Acknowledgements

To God, for all the inspiration received and right decisions taken.

To my family, for the support, care, encouragement and everything else, including my life. In particular, to Alfredo and Mariza (my parents, who have always supported me) and to Mabia (my aunt).

To my advisor, Professor Arndt von Staa. Your partnership has been fundamental not only for this thesis, but for my complete academic and professional lives. It has been a pleasure to work with you. I hope this thesis is just the beginning of a long story of cooperation for both academic and professional projects.

To all my colleagues at Minds at Work, for the positive exchange of ideas and discussions that contributed a lot in the experiments. In particular, to Frederico Guimarães Silva, my partner, and to Juliana Rezende, one of the best managers and counselors I have ever worked with.

To my friends, for all the support given at the moments I needed the most. In particular, to Andre Sotério, Allan Batista, Patricia Merlim and Daniela Maria.

To CNPq and CAPES, for the financial support; without which this work could not have been conducted.

To the “Departamento de Informática” of PUC-Rio and all its employees, especially Ruth, Rosângela and Alex.

Resumo

Pinto de Magalhães, João Alfredo; Staa, Arndt von. **Software Orientado à Recuperação.** Rio de Janeiro, 2009. 104p. Tese de Doutorado - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Software orientado à recuperação é construído com a perspective que falhas de hardware e software bem como erros de operação são fatos com os quais se deve conviver, pois são problemas que não podem ser resolvidos no desenvolvimento de aplicações reais e complexas. Consequentemente, qualquer software sempre terá uma chance diferente de zero de falhar. Algumas dessas falhas podem ser causadas por defeitos que podem ser removidos ou encapsulados. Uma questão chave é aumentar a detectabilidade de erros, ou em outras palavras, aumentar a auto-consciência comportamental de um software. Nesse trabalho, apresentamos os resultados da aplicação sistemática de técnicas conhecidas (design by contract, self-checking software, componentes de software, software depurável, design for testability, mock components e padrões) com o objetivo de criar software orientado à recuperação. Através da medição de cinco aplicações reais de tempo real, analisamos os efeitos da adoção dessas técnicas. Em particular, observamos o balanceamento do esforço gasto em diferentes estágios do desenvolvimento a exploramos o conceito de "redundância de raciocínio" que, além de prover uma maior detectabilidade de erros e depurabilidade, também leva ao aumento da qualidade por construção. Os resultados foram encorajadores por terem sido sistematicamente melhores do que aqueles reportados pela literatura e obtidos a um custo acessível.

Palavras-chave

Engenharia de software; software depurável; fidedignidade; corretude por construção.

Abstract

Pinto de Magalhães, João Alfredo; Staa, Arndt von (Advisor). **Recovery Oriented Software.** Rio de Janeiro, 2009. 104p. DSc. Thesis - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Recovery oriented software is built with the perspective that hardware or software failures as well as operation mistakes are facts to be coped with, since they are problems that cannot be fully solved while developing real complex applications. Consequently, any software will always have a non-zero chance of failure. Some of these failures may be caused by defects that could be removed or encapsulated. A key issue is to increase the detectability of errors, in other words, increase the self-awareness of the software's behavior. In this work, we present the results of systematically applying already well known techniques (design by contract, self-checking software, software components, debuggable software, design for testability, mock components and patterns) with the intent of creating recovery oriented software. Measuring the development of five different real-time and real world applications, we analyzed the effects of the adoption of these techniques. In particular we observed the balancing of the effort spent in different development stages and explore the "reduncancy of reasoning" concept that, as well as providing a higher detectability and debuggability, also leads to enhancing quality-by-construction. The results were encouraging since they were systematically better than those reported in the literature and were achieved at a feasible cost

Keywords

Software engineering; debuggable software; reliability; correctness by construction.

Summary

Figures

Tables