

論文審査の要旨

博士の専攻分野の名称	博 士 （ 情報科学 ）	氏名	RAO LEI
学位授与の要件	学位規則第 4 条第 1 項・ 2 項該当		
論 文 題 目			
Research on Formal Verification and Program Segment Testing for Software Reliability (ソフトウェア信頼性のための形式検証とプログラムセグメントテストに関する研究)			
論文審査担当者			
主 査	教授	劉 少英	
審査委員	教授	岡村 寛之	
審査委員	教授	岩本 宙造	
審査委員	教授	趙 建軍	
(九州大学)			
〔論文審査の要旨〕			
<p>This doctoral dissertation (this doctoral research) explores both approaches to integrating the formal method Event-B and the Labeled Transition Systems (LTS) to provide a more practical but rigorous method for software verification and to Program Segment Testing (PST) to support fault prevention in Human-Machine Pair Programming. While the integrated formal approach is suitable for verification of completed programs, the PST can be effectively used to support fault prevention in partial programs constructed during the programming process.</p> <p>After introducing the background and motivation of the research, the dissertation focuses on the discussions of the technical details for integrating Event-B and LTS and demonstrates the usability of the integrated formal approach using a case study on modeling and verification of the ARINC653 system. Further, to address the limitation of the integrated formal approach in supporting the new software development paradigm known as Human-Machine Pair Programming (HMPP), this research has also worked out the novel technique PST for automatic fault prevention during the process of HMPP. The performance of PST is assessed by means of an experiment.</p> <p>This dissertation contributes to the field of software engineering by providing new approaches to help software formal verification and fault prevention during programming, highlighting their individual strengths and limitations, and proposing practical solutions for enhancing software reliability across various contexts. The details of the dissertation are reflected in six chapters, which are summarized below.</p> <p>Chapter 1: Introduction. This chapter describes the research background and motivation, explains the research objectives and scope, and discusses limitations of formal methods and testing, and shows the outline of the entire dissertation.</p>			

Chapter 2: Literature Review. In this chapter, relevant concepts and techniques involved in formal methods and program segment testing are reviewed and the characteristics of formal approaches and testing techniques are discussed.

Chapter 3: Formal Verification for Software Reliability. This chapter presents in six sections the technical details of how formal method Event-B and LTS are integrated to provide a more practical but rigorous approach to formal verification of software systems. The concept of combined formal method is first explained, and a framework for system modeling and verification based on combined methods are then discussed. In particular, the discussions focus on the integration of Event-B and LTS.

Chapter 4: Program Segment Testing for Software Reliability. In this chapter, the new testing approach Program Segment Testing (PST) is described, including overview of PST, PST for arithmetic expressions, PST for index out of bound exceptions, experimental evaluation, threats to validity, and discussion about PST.

Chapter 5: Comparative Analysis and Discussion. This chapter explains the strengths of both the integrated formal verification technique and PST and discusses their limitations. The complementary characteristic of both formal verification and PST is also explained.

Chapter 6: Conclusion and Future Work. In this chapter, the work presented in the dissertation is summarized in terms of new contributions made and their implications in both theory and practice. Finally, future research directions in software tool development, extension of the proposed integrated framework, empirical studies, and training in the proposed techniques are presented.

以上、審査の結果、本論文の著者は博士（情報科学）の学位を授与される十分な資格があるものと認められる。

備考：審査の要旨は、1,500字以内とする。