論　文　の　要　旨

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

氏　名　　RAO　LEI

This dissertation explores the use of formal verification and Program Segment Testing (PST) to enhance software reliability. Initially, formal verification techniques, such as Event-B and Labeled Transition Systems (LTS), were proposed to ensure software correctness and reliability. These methods provide rigorous mathematical frameworks for modeling and verifying system behavior and are particularly suitable for safety-critical and completed systems or specifications. However, these techniques are less suitable for the iterative and evolving nature of software development, particularly in the context of Human-Machine Pair Programming (HMPP).

To address these limitations, this research introduces PST as a complementary technique. PST focuses on detecting runtime exceptions in both partial and entire programs during the software development process, providing real-time feedback without human intervention. Integrated within the HMPP framework, PST allows developers to identify and fix issues early, enhancing productivity and reducing debugging time.

The effectiveness of formal verification is evaluated through the detailed modeling and verification of the ARINC653 specification. Separately, the benefits of PST are demonstrated through experiments that showcase its ability to detect runtime errors early in the development cycle. This research highlights that while formal verification is powerful for ensuring system correctness in completed systems, PST offers significant advantages in iterative development environments by providing timely error detection.

This dissertation contributes to the field of software engineering by providing a comprehensive evaluation of formal verification and PST, highlighting their individual strengths and limitations, and proposing practical solutions for enhancing software reliability in different contexts.