論 文 の 要 旨

題 目　A Study on Sensitivity Approaches for Dependable Systems Design
（ディペンダブルシステムデザインのための感度分析アプローチに関する研究）

氏 名　　鄭　俊俊

Dependability is an all-encompassing definition for reliability, availability, safety and security, and is required in computer applications such as safety-critical control systems for road vehicles, airplanes and medical devices, and business-critical systems for e-commerce and financial transactions. To assure high dependability of systems, redundancy has been widely applied and plays an important role in enhancing system reliability. In general, there are two commonly-used types of system designs; component (or subsystem) redundancy and environmental redundancy. The component redundancy is the use of additional components or subsystems beyond the number actually required for the system to operate reliably, such as *k*-out-of-*n* redundant systems with spares. In the environmental redundancy, the system re-executes some of its initialization procedures to obtain a fresh environment that might in turn make the system less prone to failures, such as rejuvenation techniques that reboot the system before failures occur. In fact, redundancy increases not only the complexity of a system, but also the complexity of associated problems such as common-mode error. Thus, in order to detect the optimal design of systems, model-based analysis is important in the system design. Fault trees (FTs), reliability block diagrams (RBDs), Markov chains (e.g., discrete-time Markov chain (DTMC) and continuous-time Markov chain (CTMC)) and stochastic Petri nets (SPNs) are commonly-used techniques for model-based dependability analysis of computer systems.

One of the advantages of model-based analysis is sensitivity analysis, which can identify both dependability bottlenecks and critical parameters to improve system dependability. The sensitivity analysis plays an important role in the optimization of system in the design phase. In particular, the sensitivity analysis is effective to detect the critical components in the system. Generally, the parametric sensitivity and component importance (i.e., component-wise sensitivity) analysis are widely used sensitivity approaches to detect the design sensitivity of system. In addition, some extensive sensitivity analyses are devoted to evaluate the environmental sensitivity such as the survival probabilities in fault-tolerant systems, indicating how expected survivability would change with varying model parameters.

This thesis considers the sensitivity approaches for dependable systems design. Concretely, we consider the design sensitivity for virtualized systems (in Chapters 3 and 4) and real-time computing systems (in Chapter 5). For evaluating the environmental sensitivity, virtual machine (VM)-based intrusion tolerant systems (in Chapter 6) are taken into account. The thesis is

organized as follows.

Chapter 2 presents the preliminaries of the commonly-used techniques in model-based dependability analysis and the sensitivity analysis.

In Chapter 3, we focus on the component importance analysis regarding system availability of virtualized system design and develop a method to evaluate the importance of components. In the past literature, most of people focused on estimating the performance of an entire virtualized system such as the system availability. One of the important things in the system design is how to allocate system resources to components. To the best of our knowledge, there are a few papers to deal with such design problems of virtualized system. Our analysis can provide quantitative importance of all the components for system availability thereby formulating a resource allocation problem to improve system availability.

Chapter 4 is devoted to a novel state-of-the-art Markov-based component-wise sensitivity analysis. We apply it to the CTMC model of the live migration in a virtualized system, and reveal the component importance of live migration without using structure function.

In Chapter 5, we turn our attention to the component importance analysis of a real-time computing system in the presence of common-cause failures (CCFs). The CCFs are known as a risk factor of the degradation of system reliability in practice, and make it difficult to evaluate the component importance measures analytically. Thus it is important to evaluate the effect of CCFs especially in the real-time computing systems.

Chapter 6 discusses the survivability analysis of a VM-based intrusion tolerant system in the presence of intrusion. The survivability is the capability of a system to provide its services in a timely manner even after intrusion and compromise occur, which is the sensitivity of environmental changes.

Finally this thesis is summarized with some remarks and future works in Chapter 7.