Reliability of Component-based Software Systems: Modeling, Prediction and Improvements

Thanh-Trung PHAM

Supervisor: Assoc. Prof. Xavier DEFAGO

School of Information Science
Japan Advanced Institute of Science and Technology

June 2014

Abstract

Software systems become increasingly complex to meet the increasing requirements for software support from many different areas. In this situation, it is a significant challenge to assure the system reliability, i.e. its ability to deliver its intended service to users. The reliability of a software system during its runtime is dependent not only on its implementation but also on its usage.

Approaches in the field of component-based software reliability modeling and prediction provide the ability to predict the reliability of software systems before their operations. They build on architectural models, denoting components, transitions of control flow between them, and reliability-relevant aspects. They evaluate the models either by analysis methods or simulations in order to obtain the predicted reliability of software systems. Because of being based on the system models rather than the systems, approaches in the field can be applied at early design stages when the systems are not yet available, supporting design decisions and assisting in identifying reliability-critical parts of the system architectures.

However, existing approaches in the field are limited in their applicability because they either neglect or have only basic expressiveness for modeling several factors which influence the system reliability: (1) error propagation, (2) software fault tolerance mechanisms, and (3) concurrently present errors. Neglecting these factors leads to inaccurate prediction results. Basic expressiveness for modeling these factors likely reduces the ability to reuse the models and the support when evaluating different design variants.

This dissertation proposes the RMPI (Reliability Modeling, Prediction, and Improvements) approach, a reliability modeling and prediction approach for component-based software system, which considers explicitly error propagation, software fault tolerance mechanisms, and concurrently present errors, and supports design decisions for reliability improvements. More concretely, the approach offers the following contributions:

- *Consideration of error propagation*: The approach allows modeling error propagation for multiple execution models, including sequential, parallel, and fault tolerance execution models. The approach considers how the error propagation affects the system execution with different execution models, and it derives the overall system reliability accounting for the error propagation impact.
- *Consideration of software fault tolerance mechanisms*: The approach offers enhanced fault tolerance expressiveness, explicitly and flexibly modeling how both error detection and error handling of fault tolerance mechanisms influence the control and data flow within components. These capabilities enable modeling comprehensively different classes of existing fault tolerance mechanisms and evaluating their impact on the system reliability.
- *Consideration of Concurrently Present Errors*: The approach is the first work to support modeling concurrently present errors. With this capacity, it is possible to cover system failures caused by the concurrent presence of errors, tending to obtain accurate prediction results.

The approach provides a reliability modeling language that captures comprehensively different reliability-influencing factors into a reliability model of the system under study. The language, implemented in the RMPI schema, offers a developer-friendly modeling notation, including modeling elements for provided/required services, components, component connectors, activities, structures, etc.

The approach offers an analysis method that evaluates the system reliability model to obtain a prediction result. The method has been implemented in the RMPI tool, offering an automated transformation of the system reliability model into discrete-time Markov chains, and a space-effectiveness evaluation of these chains.

The RMPI approach has been validated in three case studies, by modeling the reliability, conducting reliability predictions and sensitivity analyses. Via these case studies, the approach has demonstrated its ability in supporting design decisions for reliability improvements and its reusability of modeling artifacts.

The approach and its contributions have been described in the "*Science of Computer Programming*" journal [PDH14] (currently accepted for publication and available in an online preprint version), the "*Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*" [PBD14], and further peer-reviewed publications [PD12, PHD12, PD13].

Keywords: Reliability modeling and prediction, error propagation, software fault tolerance mechanisms, concurrently present errors, component-based software systems.