Software Dependability Metrics and Analysis Based on AADL Error Model

Xin-ning Liu* and Hong-bing Qian**

G313, New Main Building, Software Engineering Institute
No. 37, College Road, Haidian District, Beihang University, Beijing, China
cherry523680602@sina.com, qhb@buaa.edu.cn

Abstract. To analyze the software products dependability early in the software life cycle is an important means to assure the final product quality. This paper firstly defines the rules of transforming the AADL error model into expanded Markov chain, and then builds a dependability measurement model based on AADL error model. After discussing how to use the property of Markov chain to measure the software, a method is presented to measure the software dependability as a whole combined with AADL core model. Finally an example is given to explain the use of the measurement method and to analyze the measurement results.

Keywords: AADL error model, dependability metrics, Markov analysis method, probabilistic reasoning.

1 Introduction

The research on software dependability is one of trusted computing branches and it has become an important research issue in recent years. As the complexity of embedded real-time systems increasing, how to improve software quality will be a major challenge in the future. The model-driven development can guarantee the system quality. The system model built early is directly related to the final actual system quality, and the software dependability reflects comprehensive quality attributes of a system. Therefore, to analyze software model dependability at an early stage can find the problems as soon as possible, and it consequently can improve the quality of software.

AADL (Architecture Analysis & Design Language) is a basis of the design and the implementation based on model-driven embedded system, and it supports the early analysis on the architecture and the design of system [1]. A software system model described by standard AADL (called AADL core model) can be extended by the annexes. Error Model Annex (EMA) is one of them. Currently, the research on software quality measurement based on AADL model is mainly by the method of

** Associate professor. Research area: software quality assurance, software process improvement and measurement, software testing process and test model.
transforming the AADL model into Generalized Stochastic Petri Nets or fault tree, which is used to measure the software reliability [2]. But the dependability is a comprehensive concept, so how to measure the software dependability based on AADL model from a comprehensive perspective still needs to be further studied. Therefore, this paper presents a method of measurement and analysis on software dependability based on AADL error model. First of all, by analyzing the relevant information of the error model, a semi-formal error model is transformed into formal expanded Markov chain. Then a dependability metrics model is built to measure individual component, and AADL core model which helps to measure the software dependability as a whole is introduced. At last, the result is analyzed by a simple method.

2 Transition from Error Model to Expander Markov Chain

The AADL Error Model Annex defines the statement rules and the semantic sets of the components and the connections to build error model. The Error Model Annex consists of two parts: the error model type and the error model implementation. The error model type declares a set of error states, error events and error propagations. The error model implementation declares error transitions between the states, which are triggered by events, and propagations declared in the error model type. Therefore, the transitions of the error states can be understood as stochastic automata. The error model type and error model implementation can all define the Occurrence properties for error events and error propagations. Occurrence properties specify the arrival rate or the occurrence probability of the events and the propagations. For the arrival rate, Occurrence properties specify an index value $\lambda$, and its probability density is $1-e^{-\lambda}$, for the Occurrence probability, Occurrence properties specify a decimal value from 0 to 1 [2]. Usually Occurrence properties are also used to indicate the recovery rate from error state to error-free state.

AADL with its extension annexes is a semi-formal language, so it is difficult to measure them. The formal method can describe the semantics more precisely, and it can be better used for the analysis for the model dependability, so this paper uses a method that transforms the error model into formal expanded Markov chain.

Markov chain points out the transitions from one state to another state, and the likelihood value from one state to another state is the transition probability. Through the analysis for EMA above, the error model can also points out the transitions of the states, which are the transitions from one error state to another error state, and the likelihood of the transitions from one error state to another error state can be pointed out by the Occurrence properties [3]. Therefore, the overall rules of the transition between the two models are: the error state in the error model corresponds to the state in the Markov chain, the transition between the error states corresponds to the transition between states in the Markov chain, the Occurrence properties of the transitions between error states correspond to the probabilities of the transitions between states in the Markov chain. In order to embody the information of error model, this paper puts forward an expanded Markov chain.