Pessimistic Dependability Models Based on Hierarchical Markov Chains

Martin Kohlík and Hana Kubátová
Department of Digital Design
Faculty of Information Technology
Czech Technical University in Prague
Email:{martin.kohlik, hana.kubatova}@fit.cvut.cz

The mission-critical systems with guaranteed levels of safety and reliability parameters are used in many different applications (e.g. aviation, medicine, space missions, and railway applications, etc.) with different impact to people and environment in case of their failure.

Such systems are composed of blocks based on different types of hardware (e.g. multi-core and many-core systems, programmable hardware like FPGA, etc.). Due to heterogeneous structure and different types of possible faults in different architectures and technologies, the realistic model, which has to be a base for necessary certifications of such systems, is mostly complicated. The state-explosion of such models leads to difficulties in construction at first, and secondly it leads to the inability to compute realistic values of dependability characteristics.

Therefore, the main aim of this paper is to propose a simplified dependability model and methods for easier dependability parameters computation, which will guarantee their required levels.

Dependability of a system is the ability to avoid *service failures* (situations where the behavior of the system deviates from the correct behavior) that are more frequent and more severe than acceptable.

Dependability is an integrating concept that includes the following attributes:

- *Safety* – absence of catastrophic consequences on the user(s) and the environment.
- *Availability* – readiness for correct service.
- *Reliability* – continuity of correct service.
- *Integrity* – absence of improper system alterations.
- *Maintainability* – ability to undergo modifications and repairs.

One of the most important techniques allowing improvement of dependability is redundancy. This means that if one part of the system fails, there is an alternate functional part. However, redundancy can have a negative impact on a system performance, size, weight, power consumption, and others.

There are many redundancy techniques including hardware, information, time, software redundancy, etc. We focus on hardware redundancy made by replication in this paper.

An event causing violation of safety of a system will be called a *hazard event*. The frequency of hazard events is called *hazard rate*.

Dependability models are models designed to calculate the hazard rate of a system. Models of complex systems consisting of cooperating dependable blocks may be created as coarse-grained or fine-grained. Coarse-grained models are small and simple models allowing exact calculations of hazard rate in a short time. On the other hand, they are inaccurate and do not reflect the internal structure of the system. Fine-grained models are accurate, but they can be too large, and thus the hazard rate calculation is time-consuming. They reflect the internal structure, but they grow rapidly in size when the complexity of a system (e.g. the number of blocks) increases.

Inexact models may be used to speed up the calculations. Accuracy is not crucial in case we prove that the inexact result is pessimistic. In other words, we must prove that the real system will be safer than the system modeled by the inexact model(s).

The presented *reduction* allows inexact pessimistic dependability models to be built. The method is based on reducing dependability models based on Markov chains. The reduced model contains one transition with one hazard rate only. This transition corresponds to a hazard event of the modeled part of the system.

The reduction of the Markov chain is the key step to calculate the hazard rate of the modeled system. It allows approximation of dependability models, so that hierarchical models can be built. The hierarchical models use multiple linked models to reflect the structure of a system. Multi-level hierarchy may be used to describe each level of redundancy independently. The hazard rates of the reduced low-level models are used in higher-level models. Higher-level models are also reduced and their hazard rates are used in top-level models.

The proposed hierarchical models allow us to

1) calculate the Safety Integrity Level (SIL),
2) determine, whether the hazard event can be tolerated/omitted safely (the hazard rate is lower than a limit value specified by SIL),
3) calculate hazard rates of systems containing multiple levels of redundancy.

Hierarchical models consisting of multiple small models

1) are easier to read/understand,
2) are easier to modify/manipulate,
3) allow the exponential number of states of the model to be avoided (the dependability parameters are calculated significantly faster).