Hierarchical Dependability Models Based on Markov Chains

Martin Kohlík

Department of Digital Design
Faculty of Information Technology
Czech Technical University in Prague
martin.kohlik@fit.cvut.cz

Dependability models allow calculating the rate of an event leading to a hazard state – a situation, where safety of the modeled dependable system (e.g. railway station signaling and interlocking equipment, automotive systems, etc.) is violated, thus the system may cause material loss, serious injuries or casualties. A hierarchical dependability model based on Markov chains allows expressing multiple redundancies made at multiple levels of a system decomposed to multiple cooperating blocks by Markov chains. The hierarchical model utilize decomposition, thus a complex dependability model is divided into multiple small models. The decomposed model is easier to read, understand and modify. The hazard rate is calculated significantly faster using hierarchical model, because the decomposition allows exponential calculation-time explosion to be avoided. The paper shows a method of reducing Markov chains and using them to create hierarchical dependability models. Two example studies are used to demonstrate the advantages of the hierarchical dependability models.

The calculation-time speedup is achieved at the cost of the accuracy, but accuracy is not crucial, if 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).

This paper presents a method of reducing dependability models based on Markov chains, so they contain one transition with one hazard rate only. The transition corresponds to a hazard event of the modeled part of the system.

The reduction allows inexact hierarchical models to be built. They 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 calculated from 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 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 are composed of multiple small models, so they

1. are easier to read/understand,
2. are easier to modify/manipulate,
3. allow exponential calculation-time explosion to be avoided (the dependability parameters are calculated significantly faster).

The proposed reduction method is demonstrated on a case study system containing multiple (up to 25) identical dependable blocks configured as an N-modular redundant system (NMR). Hierarchical models are used to illustrate the reduction method. The hierarchical models use 2 linked models (a top NMR model and a model of the internal redundancy of the block) containing up to 19 states in total, instead of up to tens of thousands states of the exact model that would result from the Cartesian product of all models.

The results indicate that the hazard rate calculated using the hierarchical model is higher than the hazard rate calculated without hierarchy (up to 33% times in the case study system presented in this paper), but the CPU-time spent on the reduction of the hierarchical model is greatly reduced (up to 40 times compared to the same system modeled by a standard non-hierarchical model).

As experiments show, the CPU-time spent on solving the system of the differential equations of the dependability model generated by the Cartesian product of the dependability models of the blocks grows exponentially with the number of blocks used, but the CPU-time spent on solving the system of the differential equations of the hierarchical dependability model is nearly constant.