HIERARCHICAL DEPENDABILITY MODELS BASED ON MARKOV CHAINS

Martin Kohlík
Informatics, 4-th class, full-time study
Supervisor: Hana Kubátová

Faculty of Information Technology, CTU in Prague
Thákurova 9 160 00 Prague 6

martin.kohlik@fit.cvut.cz

Abstract. This paper presents the structure of the dissertation thesis concerning two main topics. The first one is about the partial duplication – a method allowing the improvement of the fault coverage of the system based on dependable blocks implemented in FPGA (Field-programmable gate array). This method uses fault simulation to determine which part of the block that will be duplicated to obtain improvement of the fault security at the low overhead cost. The block-based design requires a dependability model able to take multiple levels of dependability improvements into account. There are models capable to deal with multiple levels of dependability improvements, but their capabilities are limited. A new hierarchical models based on Markov chains are concerned as the second and the main topic of the dissertation thesis and this paper.

Keywords. Dependability, Markov chain, model reduction, hierarchical model, fault security.

1 Introduction

The main part of this paper is the structure of the dissertation thesis. The main contributions of the thesis are

- the hierarchical Markov-chain dependability models allowing the total hazard rate of the system to be calculated,
- the reduction of the dependability models based on Markov chains allowing the hierarchical dependability models to be built,
- the partial duplication using fault simulation allowing the low-overhead improvement of the fault security to be achieved.

The systems used as railway equipment must meet dependability requirements given by the Czech and European Technical Standards. These standards define that all railway equipment systems must meet Safety Integrity Level (SIL) 4. SIL 4 means that any event whose rate is higher than 10^{-8} per hour must be taken into account during the dependability calculations. Any event whose rate is lower than 10^{-8} per hour may be neglected safely.

The main goal of the proposed models is to calculate hazard rate of the block-based systems that will be used to calculate the SIL value.

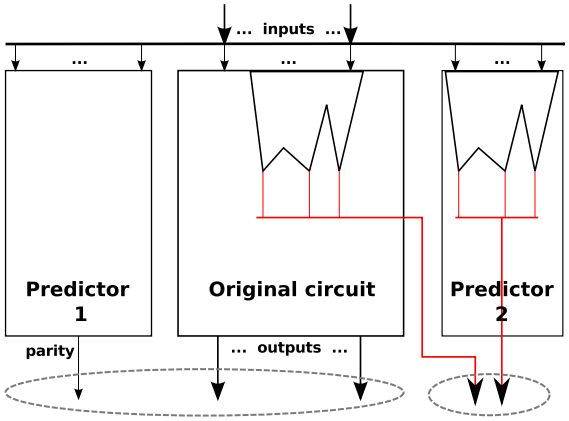

Figure 1: Partial duplication principle.

2 Markov Chains and Related Dependability Models

Markov chains (MCs) ([1] Section 6.4) are able to model systems whose events are defined by discrete probability values and are also able to model systems whose events are defined by continuous intensity rates. The second variant is more suitable to determine SIL, because the value of SIL is based on hazard rate of the modeled system.

The main advantage of Markov chains is the simple calculation of reliability function of the modeled system using the system of differential equations when all events satisfy the Markovian property. Nowadays mathematical software is able to solve such system automatically using analytic or numeric methods. The main disadvantage of Markov chain is the state explosion – the number of the states of the model grows fast when modeled system complexity is increased.

Stochastic Petri nets (SPNs) have similar properties as MCs. A complex system may be modeled by a simple SPN, but the state explosion will appear when reliability function is calculated, because the reliability function is calculated using the reachability graph equal to a Markov chain. MCs and SPNs can be transformed to each other. MC to SPN conversion is direct, SPN to MC conversion is performed trough reachability graph.

Reliability Block Diagrams (RBDs) ([1] Section 6.4) allows block-based systems to be modeled without state explosion. RBDs use hazard rates of the blocks configured as series or parallel to determine the total rate of the system, but the serial and parallel configurations are not able to model advanced redundancy techniques.

The discrete-variable models like Bayesian networks (BNs) ([1] Section 5.5) and Fault Trees (FTs) cannot deal with continuous intensity rates unless they are modified by sampling the values in time. BNs do not have the same modeling objective as Markov chains, but they can be used for dependability modeling as well, so the comparison of BN and MC should be the part of the thesis.

3 Partial Duplication

Partial duplication is the method allowing fault security of the block or the system to be increased. The detailed description can be found in [2]. This method allows Partial duplication uses two-level redundancy shown in the block scheme in Fig. 1. *Predictor1* is a parity code generator, *predictor2* is a partial copy of the circuit created on the basis of the results of the fault simulation.

The fault simulation is used to find all ”faulty” nets inside the circuit. Putting a fault (switching the logical value) on the ”faulty” net causes the change of the output values that cannot be detected by the *predictor1*. Selected ”faulty” nets are connected to newly formed test outputs and all unused logic is

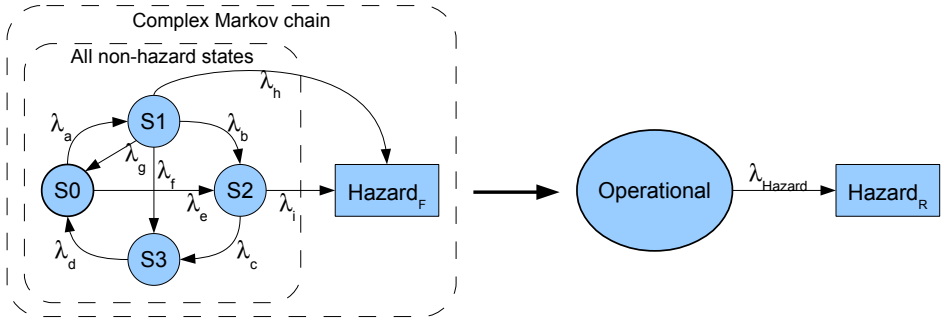

Figure 2: Illustrative example of dependability model reduction.

removed.

The method allows a balance between a fault security increment and a circuit overhead to be found. Results presented in [2] indicate that fault security increase by 1% costs ca. 1% relative overhead size of *predictor2*. If all "faulty" nets are connected to newly formed test outputs, the fault security will reach 100% (with the exceptions specified in [2]), but the overhead will be large.

The partial duplication can be modified to reduce the overhead by merging the predictors and/or using the parity code instead of comparing all the outputs. These modifications are described in [3].

Hierarchical dependability models based on Markov chains containing the models of blocks secured by partial duplication and its modifications will be presented in Section 3. These models will be used to show the impacts of increasing fault security and overhead to the hazard rate of the systems based on dependable blocks.

4 Dependability Models Reduction

The presented reduction method is intended for non-renewable Markov chains. A non-renewable Markov chain contains hazard and non-hazard states. Hazard states represent situations where safety of the modeled system is violated.

The reduction of a dependability model is made by joining all non-hazard states into a single state as shown in Fig. 2. Any dependability model can be reduced using this procedure to the same reduced model shown in the right part of Fig. 2. The hazard states correspond to each other, the index "E" (Exact) is used to mark the hazard state of the exact model. The reduced model contains hazard rate λ_{Hazard} that has to be calculated.

The drawback of the reduction is the loss of accuracy. Accuracy is not crucial in our case, but we must prove that inaccurate hazard rate calculated from reduced model is pessimistic. In other words, we must prove that the real system will be safer than the system modeled by the reduced model(s). The proof is made by comparison of the reduced failure distribution function $F_R(t) = 1 - e^{(-\lambda_{Hazard} * t)}$ that must be greater than the failure distribution function $F_E(t)$ of the exact model all the time. This condition is called the **main requirement**.

The reduction is made as follows:

1. Calculate the exact failure distribution function $F_E(t)$.
2. Find an estimated value λ_{Hazard_Est}. The main goal of this step is to make a fast estimation of the hazard rate that will be used as the starting point of the next step. This value may not meet the main requirement, but the better is the estimation, the faster will be the next step.
3. Make correction of λ_{Hazard_Est} to satisfy the main requirement. The goal of the correction is to find the lowest value of λ_{Hazard_Est} whose $F_R(t)$ meets the main requirement with the given accuracy.

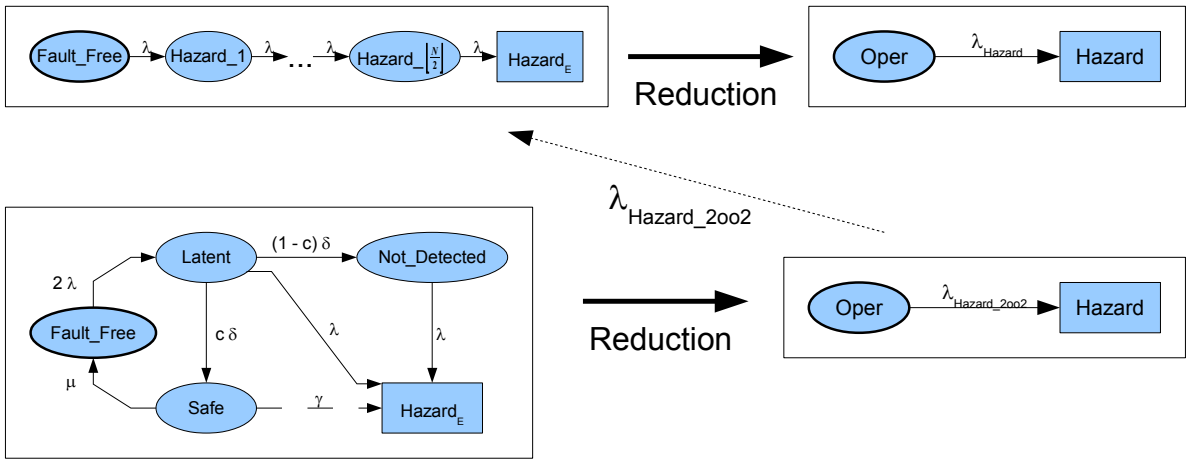

Figure 3: Principle of hierarchical dependability models based on Markov chains using multi-level hierarchy of dependable blocks.

5 Hierarchical Markov Chain Models

Hierarchical dependability models based on Markov chains (HDMCs) offer a new method to avoid the state explosion. They use hazard rates of the blocks to determine the total rate of the system in the same way as RBDs, but they allow modeling advanced redundancy techniques of the blocks in the same way as Markov chains.

It is also possible to combine HDMC and RBD because both types of models require the block to be characterized by a hazard rate and the results of both models are hazard rates of the system (or a subsystem when multiple levels of hierarchy are used).

HDMCs allows us to use multiple small models instead of one large complex model, so

- they are easier to read/understand,
- they are easier to modify/manipulate,
- the hazard rates are calculated faster.

The principle of HDMCs is shown in Fig. 3. The low-level model is the model of two-out-of-two (2oo2) system (more details of this system can be found in [4]), the top-level is the generic model of N-modular redundant system (NMR). *Reduction* is the crucial step allowing estimation of the hazard rate of the complex Markov chain. The principle of the reduction is described in Section 4.

6 Results

The proposed reduction method and the capabilities of HDMCs is demonstrated on a case study system containing up to 25 identical redundant blocks configured as N-modular redundant system (NMR) in this paper. The HDMC uses 2 linked models (a top NMR model and a model of the block) containing up to 19 states in total (top-level model – up to 14 states; the model of the block – 5 states), instead of up to tens of thousands states of exact model that would be result of Cartesian product of all models.

The HDMC of this system is shown in Fig. 3 in Section 5.

Table 1 shows the part of the comparison of runtimes results. The first column shows number of the 2oo2 blocks, the second column shows number of the states of the Cartesian model without state merging. A dependability model without state merging would be used, if the blocks were not identical. The third column shows number of the states of the Cartesian model after state merging, the fourth column shows

Table 1: Number of states and CPU-times of solutions of N-modular redundant system based on identical two-out-of-two blocks.

NMR blocks	No. of states before merging	No. of states after merging	NDSolve time [s]	Reduction time [s]
n1 (2oo2)[1)]	5	5	0.031	11.14 [2)]
n3	84	34	0.078	22.45
n5	1360	121	0.280	22.79
		...		
n25	1.501×10^{15}	22386	969.8	22.87

[1)] NMR containing one block is equivalent to a single 2oo2 block.
[2)] Contains time to reduce a 2oo2 block only.

CPU-time spent on solving the Cartesian model exactly and the fifth contains sum of CPU-times spent on reducing HDMC.

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

The results also show that the CPU-time[1] spent on solving the system of the differential equations of the dependability model generated by the Cartesian product of the dependability models of the 2oo2 blocks configured as NMR grows exponentially with respect to the number of 2oo2 blocks used, but the reduction time is nearly constant.

The plot shown in Fig. 4 shows the comparison of the failure distribution functions of the NMR based on 25 identical 2oo2 blocks. The reduction of this system (NMR25) is the most inaccurate of the systems presented in this paper, because the shape of the exact failure distribution function of NMR25 system differs from the shape of the exponential function used by the reduction widely.

The horizontal axis of the plot shown in Fig. 4 represents the time of operation measured in hours, the vertical axis represents failure distribution function. The thick dashed line represents the exact failure distribution function, the gray line represents reduced failure distribution function calculated using the Cartesian model and the black line represents the reduced failure distribution function calculated using the hierarchy model.

HDMCs including the models of blocks secured by partial duplication and its modifications presented in Section 3 will be used to show the impacts of increasing fault security and overhead to the hazard rate of the systems based on dependable blocks.

7 Conclusions

The presented dissertation thesis is focused to two topics:

- **The partial duplication** method allowing the improvement of the fault coverage of the system based on dependable blocks implemented in FPGA. This method uses fault simulation to determine which part of the block that will be duplicated to obtain improvement of the fault security at the low overhead cost. The method allows a balance between a fault security increment and a circuit overhead to be found. Results indicate that fault security increase by 1% costs ca. 1% relative overhead size of *predictor2*. If all "faulty" nets are connected to newly formed test outputs, the fault security can reach 100%.

[1]NDSolve command of Mathematica 8.01 [5] software running on Intel Core i5 @3.3 GHz, OS: Win7 64-bit

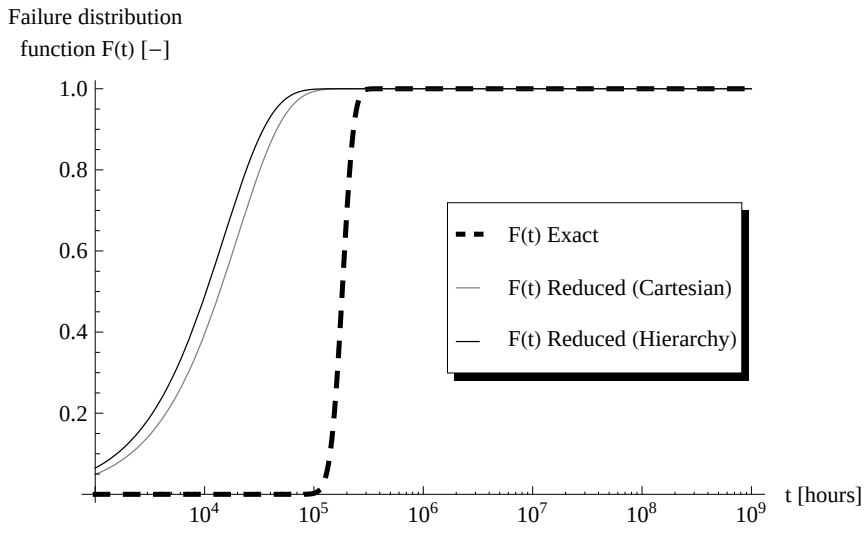

Figure 4: Comparison of failure distribution functions of N-modular redundant system based on 25 identical two-out-of-two blocks.

- **The hierarchical dependability models** based on Markov chains and **reduction of Markov chains** allowing the hierarchical dependability models to be built. The hierarchical models can be used to calculate hazard rate – rate of hazard event that will lead to situation situations where safety of a system is violated. The results indicate that the hazard rate calculated using hierarchical dependability models based on Markov chains is higher than the hazard rate calculated without hierarchy (by 33% in the worst case study system presented in this paper), but the CPU-time spent on the reduction of the hierarchical dependability models based on Markov chains is greatly reduced (up to 40 times compared to the same system modeled by a standard non-hierarchical model). The results also show that 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 respect to 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.

Acknowledgment

This research has been partially supported by the project SGS12/094/OHK3/1T/18.

References

[1] Electronic Reliability Design Handbook – MIL-HDBK-338. Web: `https://assist.daps.dla.mil/quicksearch/basic_profile.cfm?ident_number=54022`

[2] Borecký, J., Kohlík, M., Kubátová, H and Kubalík, P.: Faults Coverage Improvement based on Fault Simulation and Partial Duplication, In Proc. of 13th Euromicro Conference on Digital System Design, Los Alamitos: IEEE Computer Society (2010), pp. 380–386.

[3] Borecký, J., Kohlík, M. and Kubátová, H.: Miscellaneous Types of Partial Duplication Modifications for Availability Improvements, To be published In Proc. of 15th Euromicro Conference on Digital System Design.

[4] Kohlík, M. and Kubátová, H.: Reduction of Complex Safety Models based on Markov Chains, In Proc. of the 2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), New York: IEEE Computer Society Press (2012), pp. 183–186.

[5] Wolfram Mathematica web page. `http://www.wolfram.com/mathematica/`