Reduction of Complex Safety Models based on Markov Chains

Martin Kohlík and Hana Kubátová
Department of Digital Design
Faculty of Information Technology
Czech Technical University in Prague
Thákurova 9, 160 00 Prague 6, Czech Republic
Email: {martin.kohlik, hana.kubatova}@fit.cvut.cz

***Abstract*—This paper presents a method how to reduce safety models based on Markov chains. The safety model is used to calculate the probability and rate of an event leading to the hazard state – situation, where safety of a modeled system is violated, so the system may cause material loss or mortality. The reduction method allows us to prove that the rate of the event is sufficiently small hence the hazard state may be neglected. The real safety model of railway station signaling and interlocking equipments is used as a case study.**

I. Introduction

We design railway equipment systems based on Field Programmable Gate Arrays (FPGAs) composed of cooperating modules at our department. [1], [2], [3]

FPGA-based systems are sensitive to many effects that can change their programmed function. [4] These changes are most unwelcome in systems, where the material loss or mortality can be caused because of their failure. The improvement of dependability parameters of a final design is required to minimize the impact of such effects.

The dependability of a system is the ability to avoid service failures (situation when the delivered service deviates from correct service) that are more frequent and more severe than is acceptable. [5]

Dependability is an integrating concept that includes Safety, Availability, Reliability, Integrity and Maintainability. We focus on Safety parameter in this paper. Safety is defined as absence of catastrophic consequences on the user(s) and the environment. [5]

One of the most important design techniques allowing improvement of dependability is redundancy. We focus on hardware redundancy made by replication of hardware in this paper, but there are other redundancy techniques like information, time, software redundancy etc. [6]

We also need to prove that the final design using selected redundancy technique meets dependability requirements given by the Czech Technical Standard ČSN 50129 [7] in accordance with the European Standard EN 50129:2003 [8].

These standards are focused on railway equipment systems classified as the safety-critical systems. These standards define that safety-critical 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 omitted safely.

If an event causes a situation where safety of a system is violated, it will be called *hazard event*. A rate of a *hazard event* is called *hazard rate*.

Safety models based on Markov chains are designed to calculate a hazard rate of a system. This paper presents a method of reducing safety models that allows us to reduce the models, so they contain one transition with one hazard rate only. The transition corresponds to hazard event of the system.

The proposed reduction method allows us to

1) calculate Safety Integrity Level (SIL) (Top-level model reduction),
2) determine, whether the hazard event can be tolerated/omitted safely (The hazard rate is lower than a limit value specified by SIL.).

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 reduced model.

The proposed reduction method is used to determine hazard rate of a case study system containing two modules in this paper.

The paper is organized as follows: Section II introduces absorbing Markov chains and basic reliability functions. Section III shows the safety model reduction process. The reduction procedure is applied on the case study system in Section IV. Section V concludes the paper.

II. Theoretical Background

The presented reduction method is intended for absorbing Markov chains. [9] Absorbing Markov chain contains hazard (absorbing) and non-hazard states. Hazard states represent situations where safety of a system is violated. There are paths from each non-hazard state leading to a hazard state and there are no paths leading from a hazard state to a non-hazard state.

The reduction uses failure distribution function in its final step. Failure distribution function $F(t)$ is a complementary function of reliability function. Reliability function $R(t)$ is a probability that the system will perform its intended function

under specified design limits from time 0 until time t at least. [5], [10]

The mathematical definition of a hazard rate is that the hazard rate λ_{Hazard} is a constant failure rate. Failure rate $f(t)$ is a conditional probability of failure density function. The condition is that the failure has not occurred until time t. [10]

Mean Time To Failure (MTTF) is mean time until a failure of a system. [10] MTTF is given by

$$MTTF = \int_0^\infty t\, f(t)\, \mathrm{d}t = \int_0^\infty R(t)\, \mathrm{d}t \qquad (1)$$

Consider the exponential distribution where reliability function is given by

$$R(t) = e^{-\lambda_{Hazard}\, t}$$

then MTTF is

$$MTTF = \int_0^\infty e^{-\lambda_{Hazard}\, t}\, \mathrm{d}t = \frac{1}{\lambda_{Hazard}} \qquad (2)$$

Absorbing Markov chain may be used to calculate MTTF of a system. MTTF is calculated by applying the Laplace transform over the differential equation system derived from the Markov chain. The method of generating of the differential equation system and the method of calculation of MTTF using the Laplace transform are described in [11].

III. Reduction of Safety Models

The reduction of the safety model is made by joining all non-hazard states into a single reduced state as shown in Fig. 1. Any non-renewable safety model can be reduced using this procedure to the same reduced model shown in Fig. 1. The hazard states correspond to each other, the indices "E" (Exact model) and "R" (Reduced model) are used in further calculations to distinguish among them. The reduced model also contains hazard rate λ_{Hazard} that has to be calculated.

The reduction is valid when the **main requirement** is met. The main requirement is that the failure distribution function $F_R(t)$ of reduced model must be greater than the failure distribution function $F_E(t)$ of exact model all the time.

The reduction is made as follows:

1) Calculate MTTF of system using Laplace transformation over the differential equation system derived from the Markov chain.
2) Use MTTF to obtain estimation of λ_{Hazard} using equation (2) from Section II. Equation (2) can be used, because reliability function of the reduced model has the exponential distribution.
3) Calculate the failure distribution function $F_E(t)$ of the exact model.
4) Make correction of λ_{Hazard} to satisfy the main requirement. The correction coefficient k is used during correction. It is incremented by 0.1, but any positive increment can be used. The lower value of increment leads to more accurate result, but it increases the number of iterations.

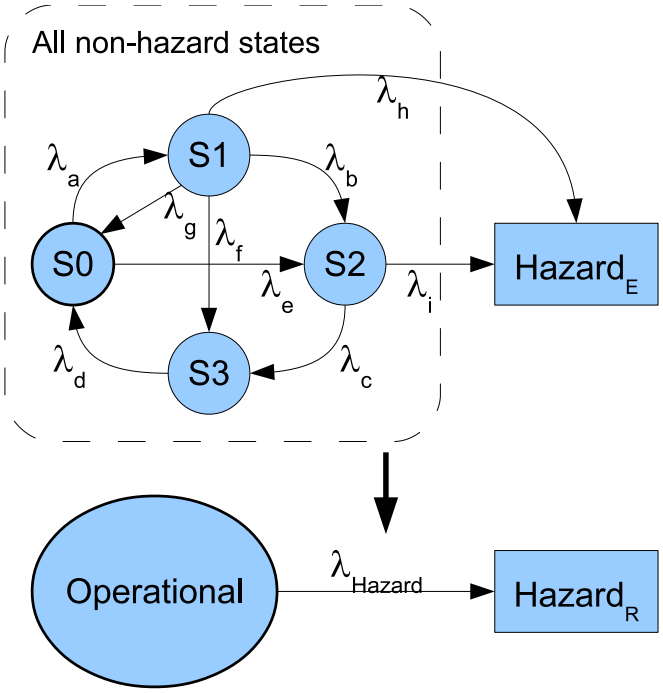

Fig. 1. Illustrative example of safety model reduction.

The correction algorithm:

```
k = 1;
F_R(t) = 1 - e^(- lambda_Hazard * t)
while (main requirement not met) {
k = k + 0.1;
lambda_Hazard_Corrected =
   k * lambda_Hazard;
F_R(t) = 1 -
   e^(- lambda_Hazard_Corrected * t);
}
```

IV. Case Study System

A. System Description

The Two-out-of-two system (2oo2) is a system containing two independent functional parts that meets the following requirements:

- The safety of the system cannot be violated by a single fault in the system.
- Two faults will never occur in the system at the same time.
- Assuming a fault occurs in one module, the redundant module is able to lock the system into a safe state, so that a possible future fault will not cause a hazard state. Safe state is considered as the situation where the system is not operational, but the safety is not violated (e.g. all lights are red and traffic is operated by human operator).
- If the second fault occurs before the redundant module locks the system, the safety of the system may be violated. This double-fault situation is considered as the hazard state.

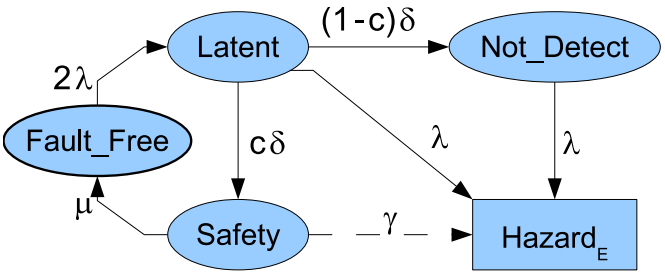

Fig. 2. Markov chain of the Two-out-of-two system used to calculate the exact-model failure distribution function.

This model is currently used as a safety model of the railway station signaling and interlocking equipments [12].

B. Exact Safety Model

The model shown in Fig. 2 is used to calculate the exact-model failure distribution function $F_E(t)$ of the Two-out-of-two (2oo2) system.

The description of the states and the arcs in Fig. 2:

- $Fault\_Free$ – the functional/fault-free state of the system
- $Latent$ – the system contains a fault that has not been detected yet
- Not_Detect – the system failed to detect the first fault
- $Safety$ – the fault has been detected – the system is locked in the safe state
- $Hazard_E$ – the second fault has appeared – the hazard state

- $2\,\lambda$ – the fault rate of the first fault (the fault can affect two functional parts)
- $(1-c)\,\delta$ – the self-test rate (δ) combined with the probability that the fault is not detected $(1-c)$
- $c\,\delta$ – the self-test rate (δ) combined with the probability that the fault is detected (c)
- μ – the repair rate
- λ – the rate of the second fault affecting the unaffected functional part. (The second fault hit inside already affected functional part cannot cause a hazard, because the second functional part works correctly.)
- γ – the human operator's hazard behavior rate. (This rate should be included into the safety analysis if a more complex analysis needs to be done.)

C. Reduced Model Parameter Calculation

The reduced model of the 2oo2 system is the same as shown in illustrative example in Fig. 1.

The steps of reduction corresponds to algorithm shown in Section III.

1) Calculate MTTF:
   a) Generate system of differential equations:

$$
\begin{aligned}
p'_{Fault\_Free}(t) &= p_{Safety}(t)\,\mu - p_{Fault\_Free}(t)\,2\lambda \\
p'_{Latent}(t) &= p_{Fault\_Free}(t)\,2\lambda - \\
&\quad p_{Latent}(t)\,((1-c)\,\delta + c\,\delta + \lambda) \\
p'_{Not\_Detect}(t) &= p_{Latent}(t)\,(1-c)\,\delta - \\
&\quad p_{Not\_Detect}(t)\,\lambda \\
p'_{Safety}(t) &= p_{Latent}(t)\,c\,\delta - p_{Safety}(t)\,(\mu+\gamma) \\
p'_{Hazard_E}(t) &= p_{Safety}(t)\,\gamma + p_{Latent}(t)\,\lambda + \\
&\quad p_{Not\_Detect}(t)\,\lambda \\
p_{Fault\_Free}(0) &= 1 \\
p_{Latent}(0) &= p_{Not\_Detect}(0) = 0 \\
p_{Safety}(0) &= p_{Hazard_E}(0) = 0
\end{aligned}
$$

   b) Use Laplace transformation to calculate MTTF.
2) Use equation (2) from Section II to calculate estimation of λ_{Hazard}:

$$\lambda_{Hazard} = \frac{2\,\lambda\,(\gamma\,\delta + \gamma\,\lambda + \delta\,\mu - c\,\delta\,\mu + \lambda\,\mu)}{3\,(\delta+\lambda)\,(\gamma+\mu) - 2\,c\,\delta\,(\gamma - \lambda + \mu)} \quad (3)$$

3) Solve system of differential equations generated in the first step using any analytic or numeric method.
4) Make correction.[1]

D. Results

The probability of the detection of a fault, the fault rate, the self-test rate of the case study system form the following parameters values. The values have been taken from [13]. All rates are per hour.

$\mu = 24^{-1}$ – the repair rate
$\lambda = 10^{-5}$ – the fault rate
$\delta = 10^{-1}$ – the self-test rate
$c = 0.6$ – the probability of detecting a fault by the self-test
$\gamma = 10^{-3}$ – the human operator's hazard behavior rate

These values and the equation (3) shown in Section IV-C form up the estimated value of λ_{Hazard}:

$$\lambda_{Hazard} = 4.6 \times 10^{-6}$$

The plot shown in Fig. 3 shows the exact-model failure distribution function, the reduced failure distribution function and the reduced failure distribution function using the corrected value of $\lambda_{Hazard\_Corrected}$. The horizontal axis represents the time run measured in hours, the vertical axis represents failure distribution function. The dashed line represents the exact-model failure distribution function, the dot-dashed line represents the reduced failure distribution function. The area, where the exact-model failure distribution function is greater than the reduced failure distribution function, is highlighted by grey coloring. The solid line represents reduced failure distribution function using corrected value $\lambda_{Hazard\_Corrected}$.

[1]Correction requires all rates used in the exact safety model to be specified. Full specification and correction is done in the following section (Section IV-D).

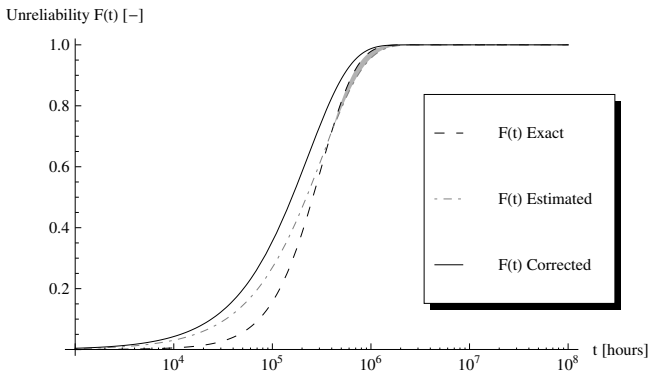

Fig. 3. Exact-model and reduced failure distribution functions of Two-out-of-two system.

As you can see, there is the area, where exact-model failure distribution function is greater than reduced failure distribution function. The correction of the estimated value of λ_{Hazard} is necessary in such case.

The correction constant $k = 1.7$ is sufficient in this case (see iteration algorithm in Section III), so the corrected value of λ_{Hazard} is

$$\lambda_{Hazard\_Corrected} = 7.82 \times 10^{-6}$$

The estimated rate of a double fault of the system exceeds 10^{-8}, so a double fault event cannot be neglected in this case. This system does not meet SIL 4, thus it cannot be used in safety-critical railway equipment.

Two-out-of-two system can be integrated to a complex system as a module. If the complex system uses another redundant module, the rate of a double fault will decrease and the complex system will meet SIL 4.

V. Conclusions

The proposed method of reduction of safety models based on Markov chains 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 reduction is intended for any safety model – absorbing Markov chain satisfying the conditions mentioned in Section II. The estimation is especially useful when it allows us to prove that the hazard rate of a system is low enough to meet Safety Integrity Level requirements, so a hazard event may be neglected in the further models and calculations.

The hazard rates of reduced models are also useable in hierarchical safety models that are currently developed at our department. Hierarchical models use multiple linked models to reflect a structure of a system. Multi-level hierarchy may be used to describe multiple level of redundancy independently and to decompose one safety model of a complex system into multiple smaller models.

The reduction is used to estimate the rate of a double fault in the Two-out-of-two system that is used as the safety model of the railway station signaling and interlocking equipments.

The double fault rate of the Two-out-of-two system is 7.82×10^{-6} per hour, so the system with parameters presented in Section IV-D does not meet Safety Integrity Level 4. A double fault must be taken into account in this case, but the reduced model can be used when the complex system built from Two-out-of-two modules is created. The double fault rate may be decreased using additional redundancy, so a double fault might be neglected in such complex system safely. The rate of a double fault of such complex system can be calculated by Fault Tree Analysis or hierarchical models.

The reduction procedure will be improved to support multi-hazard systems. The multi-hazard system can fail in more than one way (e.g. a diode that may be opened or shorted). Different failure types may cause the different behavior of the system, so they cannot be merged. This improvement will allow us to create the detailed models of large complex systems and to simplify them safely in accordance with Czech and European standards.

Acknowledgment

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

References

[1] Borecký, J., Kubalík, P. and Kubátová, H.: Reliable Railway Station System based on Regular Structure implemented in FPGA, In Proc. of 12th Euromicro Conf. on Digital System Design, Los Alamitos: IEEE Computer Society (2009), pp. 348–354.

[2] Kubalík, P., Dobiáš, R. and Kubátová, H.: Dependable Design for FPGA based on Duplex System and Reconfiguration, In Proc. of 9th Euromicro Conference on Digital System Design, Los Alamitos: IEEE Computer Society (2006), pp. 139–145.

[3] Kubalík, P. and Kubátová, H.: Dependable design technique for system-on-chip, Journal of Systems Architecture, Vol. 2008, no. 54, (2008) 452–464. ISSN 1383-7621.

[4] Normand, E.: Single Event Upset at Ground Level, IEEE Transactions on Nuclear Science, vol. 43, 1996, pp. 2742–2750.

[5] Avižienis, A., Laprie, J.-C., Randell, B. and Landwehr C.: Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January–March 2004.

[6] Pradhan, D., K.: Fault-Tolerant Computer System Design, Prentice Hall PTR, Upper Saddle River, New Jersey 1996, ISBN 0-7923-7991-8.

[7] Czech Technical Standards ČSN EN 50129 Drážní zařízení Sdělovací a zabezpečovací systémy a systémy zpracování dat Elektronické zabezpečovací systémy (2003). http://nahledy.normy.biz/nahled.php?i=68996 (in Czech – preview only)

[8] European Standards EN 50129:2003 Railway applications Communication, signalling and processing systems Safety-related electronic systems for signalling. http://www.cenelec.eu/dyn/www/f?p=104:110:1414646381618556:::: FSP_PROJECT,FSP_LANG_ID:13550,25 (preview only)

[9] Empirical Techniques in Finance, Chapter 2: Basic Probability Theory and Markov Chains, Springer Finance, Springer Berlin Heidelberg (2005), pp. 5–17.

[10] Hoang, P.: System Software Reliability, Chapter 2: System Reliability Concepts, Springer Series in Reliability Engineering, Springer London (2007), pp. 9–75.

[11] Shooman, M.: Reliability of Computer Systems and Networks, Appendix B: Summary of Reliability Theory, Wiley (2002), pp. 411–474.

[12] Dobiáš, R.: Methodology of Fail-safe and Fault Tolerant System Design, Doctoral Thesis, CTU in Prague (2010).

[13] Dobiáš, R. and Kubátová, H.: FPGA Based Design of the Railway's Interlocking Equipments, In EUROMICRO Symposium on Digital System Design, Piscataway: IEEE (2004) 467–473.