Systematic Method for Constructing a Markov Model for the Safety of Systems

Mohammad Sadeghi

Computer Engineering Department, Dezfoul Branch, Islamic Azad University, Dezfoul, Iran
sadeghi.m.com@gmail.com

Abstract: In large set of dependable systems, such as aircrafts, nuclear power plants, traffic control, monitoring and controlling medical equipment, parameters of reliability and safety are immensely important. In addition to the proper functioning, these systems must be designed in a way so that in case of an error in hardware and software they would stop functioning in a safe way so that no harm would come to anybody or anything; for example an airplane would conduct an emergency landing or a power plant would perform an emergency shutdown. One of the methods to secure a system is the use of redundancy in its structure. Redundancy can be embedded in different ways into the system and the NMR form is one of the conventional methods. When a system is designed with appropriate redundancy, it must be then analyzed and modeled in terms of safety and one of the common methods is the Markov process. This paper presents a systematic method for constructing a Markov model of the safety of systems and implements it in a number of prototype systems. Furthermore, the capability of the method for the direct construction of the Markov model for the NMR system of safety is also described.

[Mohammad Sadeghi, Gholamreza Latif Shabgahi. **Systematic Method for Constructing a Markov Model for the Safety of Systems.** *Academ Arena* 2013;5(8):18-23] (ISSN 1553-992X). http://www.sciencepub.net/academia. 3

Key words: Safety, Evaluation, NMR, TMR, Markov model, Redundancy.

1. Introduction

Nowadays, safe and fault-tolerant systems play a major role in the society. A safe system is defined as a system that is able to function properly in the presence of hardware errors, software errors, disturbances imposed from outside the system or user faults and does not act in a hazardous manner. For a certain set of reliable systems such as real-time embedded systems, commercial transaction systems, transportation control systems (e.g. railways, aircraft, ships and cars) nuclear power plant control systems, military and spatial systems and chemical industries (such as environments where toxic, flammable or explosive materials exist) safety is a very important parameter. Safety is the probability that in any given time, the system either functions properly (even if a software or hardware related error occurs) or it terminates its work in a manner that is safe and free from serious danger so that no harm comes to anybody or anything. The safety of system in the moment of t is the absence and avoidance of catastrophic consequences for the users and the surrounding environment of the system in the given time range [0, t] Safety can be increased through several methods; using proper and high quality components and subsystems, utilizing internationally approved standards in the design, construction and testing phases of a system, implementing auditing and validating methods and using redundancy are among the common methods.

Applying additional resources (implementing redundancy) may occur in the areas of hardware, software, time and information. It is obvious that any redundancy in the system, the size, price, power consumption and the number of system components will increase and this is the price that must be paid in order to increase the level of safety of a system. One of the mechanisms for implementing redundancy to improve safety in systems is the usage of hardware redundancy of static type (NMR form) in which the redundant modules-parallel to each other-function on the input and present the outcome of their work to a decision maker for the judgment of their output. The decision maker which in most cases is a majority detector circuit, inspects the output of the redundancy modules and in case of observing agreement in the majority of them, it selects the agreed number as the final output of the system. [2, 10, 11]. It is obvious that his system is safe as long as:

Most of its modules properly agree on a number, and if an agreement is not reached for the output of the majority of modules, then the next module of the system must be disabled in a safe and non-hazardous manner.

The Markov method can model and evaluate the system in order to inspect its safety. A systematic method for constructing the final Markov model of the safety of systems has been presented in this paper. We will describe the method in the form of an example and apply it for a number of other reliable systems. This paper is organized as follows: The second section briefly describes the Markov model. The third section describes the proposed systematic method for the construction of the Markov model of safety of systems and demonstrates its accuracy by the use two examples. The fourth section examines the process of direct construction of Markov model for NMR systems for safety by using the findings in section three and with a brief word the fifth section ends the paper.

2. Morkov Model

The Markov model was first introduced by a mathematician of the same name in the late 1960s. Markov proposed a particular mathematical model for the systems in which the future state of the system only depended on the present state and not on its past state. The "memoryless" property which is called the "Markov property" states that in case of the occurrence of defect, disorder and repair, the system passes from one state to the other and depending on the type of the system, this passing may have a fixed or variable rate [6]. The Markov model presents useful methods for evaluating the performance, reliability, availability and safety of the system. Furthermore, it models the independent and dynamic connections between the components of the system in a simple way. This model is used to assess the long-term reliability and safety of equipment that possess defined strategies of repair and maintenance and also to determine the "range of repair and inspect" of a system [8, 10]. Among the advantages of this model in comparison to hybrid modeling techniques, we can mention the simple modeling approach, the modeling of a newly configured system due to faults, modeling of the faulty components and the ones insulated against defects, complex modeling of repair and maintenance, modeling of complex systems and well-ordered events [2, 4, 5, 6].

The Markov model can be illustrated based on the definition of the reliability and safety of systems [3]. The constructed model is analyzed and the output of the model which is the amount of a number for the reliability or safety of the system is calculated [1].

3. Introducing a Systematic Method to Draw a Markov Model for the Safety of Systems

A. *Single component safety model*

In order to draw the Markov model for the safety of systems, by utilizing the definition of safety and in accordance with Fig. 1, two states will be considered for each component:

1. The mode in which the component is disabled in a 'safe' way. In this mode, the system is disabled but it does not harm the people or the surrounding environment and valuable objects.
2. The mode in which the component is disabled in an 'Un-safe' way. In this mode, the component shows hazardous manners and harms the people and its surrounding environment.

Thus, in drawing the Markov model of the safety of system, the two distinct modes of *FU* and *FS* for disabling the components of that system must be defined.

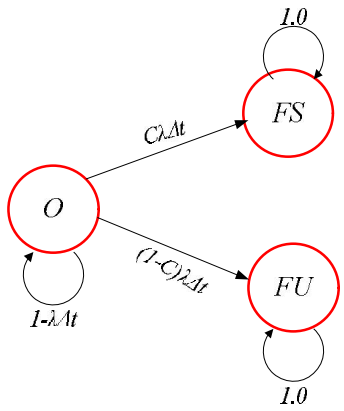

Fig. 1. The Markov of safety of a simple module.

In this figure, *C* is the probability that the system would reach the disability mode of *FS*. The safety mode of the system *S(t)* according to Markov is calculated as follows:

$$S(t) = P_O + P_{FS} = 1 - P_{FU} \qquad (1)$$

In the recent connection, P_o is the safe mode of the system, P_{FS} is the probability of the safe disability of the system and P_{FU} is the probability of the unsafe disability of the system. It is evident that the probability of the safety of the system in any instance is calculated by the adding the probability of safe modes and the safe disabling mode of the system.

B. *Stating the method for drawing the Markov model for safety*

We consider the model in Fig. 1 for a single component as the base model and describe the systematic method below for constructing the Markov model for the safety of a system. In order to simplify the understanding of the description, we shall explain the method through the use of TMR form (a specific mode of the NMR system when *n=3*). For the sake of simplicity, normally decision maker is considered to be ideal and we assume that:

1. The system starts functioning from the initial safe mode.
2. In any given instance, only one module can be defected and therefore the occurrence of two simultaneous and further defects is not possible.
3. Repair and maintenance does not exist in the system.

The proposed systematic method draws the Markov model for safety in four steps

Step 1. According to Fig. 2, the system starts to function with three intact modules. After some time, as a result of the occurrence of a defect one of the modules with the probability of *C* is disabled in a "safe" way and is transferred to mode *2-FS*. Therefore, with the probability of

(*1-C*) it is disabled in an "Un-Safe" way and enters the *2-FU* mode.

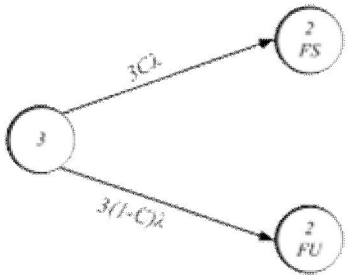

Fig. 2. A defect in one of the modules in the TMR system..

Step 2. Now the system is in of the two modes of *2-FS* or *2-FU*. Again with the probability of *C*, it is transferred from the *2-FS* mode to *1-FS-FS* and with the probability of (*1-C*) it is transferred to *1-FS-FU*. The very same mode of transference occurs in the mode of *2-FU* (Fig. 3).

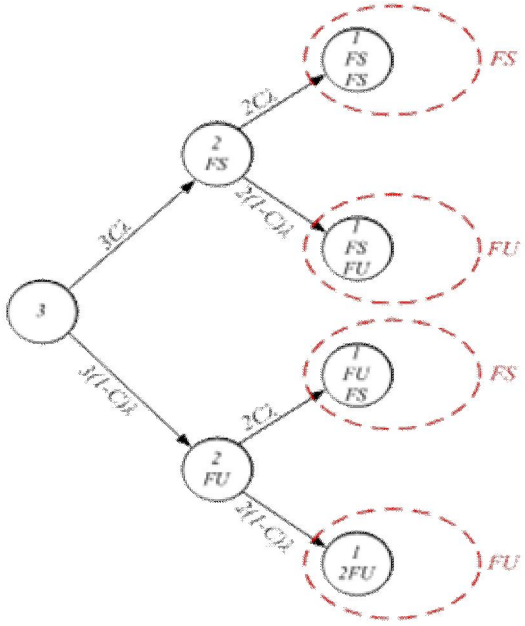

Fig. 3. A defect in the second module in the TMR system.

Step 3. We conduct the process in Section B for each and every new mode and we continue until the number of the intact modules drop to below *(n+1)/2* (n is the number of modules in the NMR system). At this point the "type" of the last modes must be determined (*FU* or *FS*). In order to determine the type of the mode, we must simply observe the manner with which the last module is disabled.

- If the module was last disabled in a "safe" way, we will consider its mode to be "safe".
- If the module was last disabled in an "Un-safe" way, we will consider its mode to be "Un-safe".

Fig. 4 demonstrates this method of applying "type" to mode.

Fig. 4. Applying the final type of mode of module in the last Algorithm.

Thus, the Markov model for safety of TMR system is formed as demonstrated in Fig. 5.

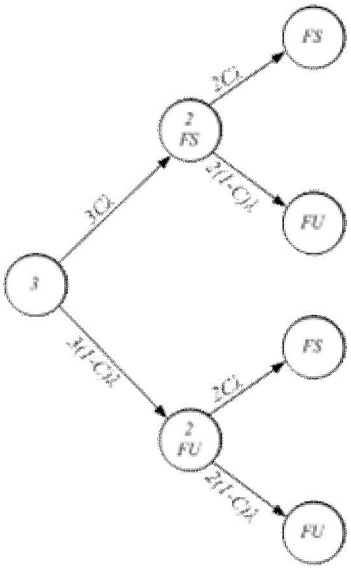

Fig. 5. The un-simplified final Markov model for safety of TMR system.

Step 4. In this stage, by combining the modes of *FS* with each other, and *FU* with each other, the Markov model is simplified (Fig. 6).

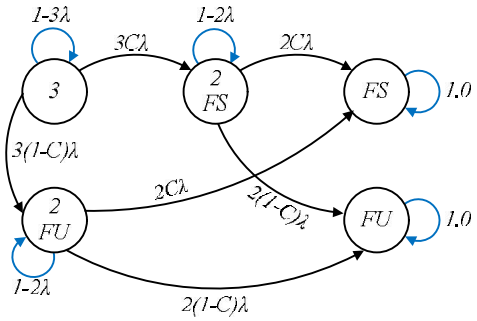

Fig. 6. The simplified final Markov model for safety of TMR system.

C. Drawing the Markov model for safety by the use of the proposed systematic method

In this section, we implement the above method to draw Markov model for safety of the 5MR and 7MR systems and we draw their Markov models. It should be noted that to this date, there has been no mention of these models in books and references.

C-1. Drawing the Markov model for the safety of 5MR system.

This system will produce an output if 3 modules out of the 5 modules function properly. The Markov model for safety of this system that has been constructed based on the proposed systematic method of this paper are demonstrated in Fig. 7 and 8.

It can be observed that the final Markov model for the safety of 5MR system contains (*5+1*) distinct modes that are organized in two lines. The first line consists of *4* modes in which the modules are disabled in a "safe" way and the second line consists of *3* modes in which the modules are disabled in an "Un-safe" way.

C-2. Drawing the Markov model for the safety of 7MR system.

This system will produce an output if *5* modules out of the *7* modules function properly. The initial Markov model is demonstrated in Fig. 9 and the final Markov model which contains (*2+7*) modes is demonstrated in Fig. 10. Also the final Markov models of 9MR and 11MR are shown in Fig. 11 and 12 respectively.

The first line of the final model consists of *5* modes in which the modules are defected in a safe and gradual manner and the second line consists of *4* modes in which the modules are disabled in an "Un-safe" and hazardous manner.

D. Using the mentioned systematic methods for independent drawing of final Markov model for the safety of NMR systems.

One of the advantages of the mentioned systematic methods for drawing the Markov model for the safety of NMR systems is that the final Markov model for safety can be directly drawn (without drawing the initial model). By closely observing the mentioned final models of TMR, 5MR and 7MR in the third section of this paper and by considering the points below, the reader can easily draw the models:

- The Markov model for the safety of NMR system contains (*N+2*) modes that are organized in two lines. The first line consists of the intact mode and the fail-safe modes that are *(N+3)/2* in number. The second line consists of the gradual defect of "Un-safe" modules which add up to *(N+1)/2*.
- From all the modes in the first line (except for the last mode of that line) to the modes of the second line, certain transferences with the probability ratio of (*1-C*) exist (meaning that the first mode of the first line is transferred to the first mode of the second line - the second mode of the first line is transferred to the second mode of the second line and…).
- From all the modes in the second line (except for the last mode of that line) to the modes of the first line (except for its first two modes) certain transferences with the probability ratio of *C* occur (meaning that there is a transference from the first mode of the second line to the third mode of the first line - from the second mode of the second line to the fourth mode of the first line and …).

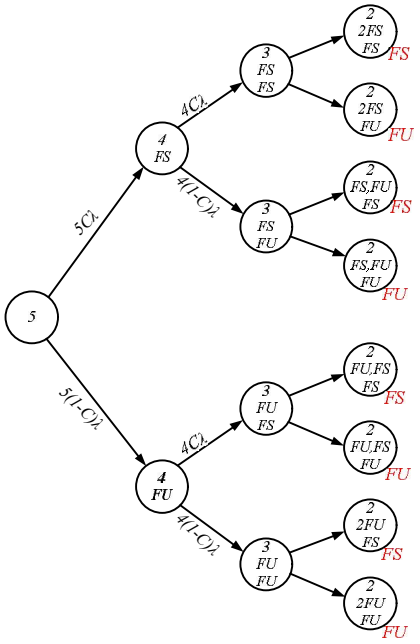

Fig. 7. The initial Markov model for the safety of 5MR system.

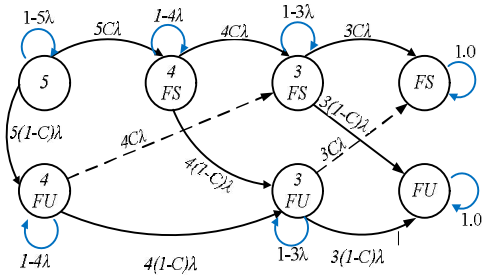

Fig. 8. The final Markov model for evaluating the safety of 5MR.

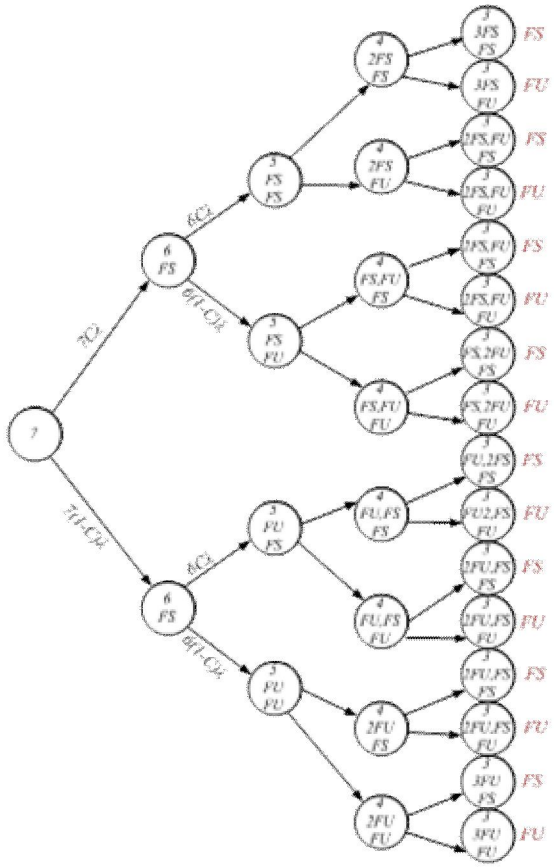

Fig. 9. The initial Markov model for the safety of 7MR system.

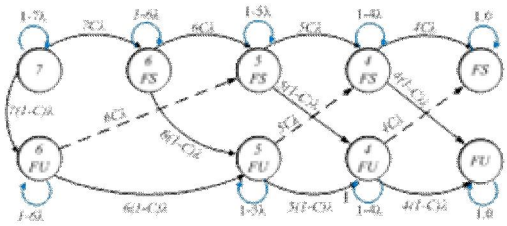

Fig. 10. The final Markov model for evaluating the safety of 7MR.

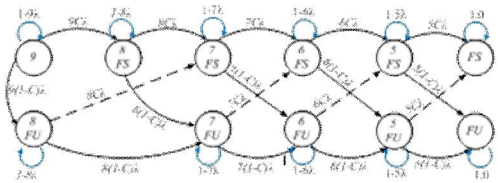

Fig. 11. The final Markov model for evaluating the safety of 9MR.

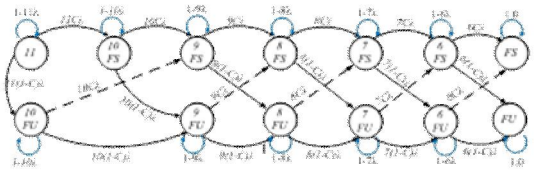

Fig. 12. The final Markov model for evaluating the safety of 11MR.

4. Conclusions

Based on the research and studies of the authors of this paper, to this date no method has been introduced for the systematic drawing of the Markov model of the safety of systems. In this paper, a systematic method for the Markov model of the safety of systems has been proposed and by its usage, the model of the TMR, 5MR, 7MR, 9MR and 11MR systems were drawn. Subsequently, by utilizing the drawn models, a general method for drawing the final Markov model for NMR systems was introduced.

Author:
Mohammad Sadeghi
Computer Engineering Department, Dezfoul Branch, Islamic Azad University, Dezfoul, Iran
sadeghi.m.com@gmail.com

References

1. B. W. Johnson, “Design & Analysis of Fault-Tolerant Digital Systems,” University of Verginia, Addison-Wesley, MA, USA, 1989.
2. M. Rausand and A. Hoyland, “System Reliability Theory: Models, Statistical Methods, and Applications,” John Wiley and Sons, 2004.
3. M. L. Shooman, “Reliability of Computer Systems and Networks: Fault Tolerance, Analysis and Design,” John Wiley and Sons, USA, ISBN: 0-471-29342-3, 2002.
4. B. Parhami, “Fault Tolerant Computing: Motivation, Background, and Tools,” URL: www.ece.ucsb.edu/~parhami/, 2007.
5. C. Krishna, “Fault-Tolerant Systems,” 1st Edition from Israel Koren, 2007.
6. D. K. Pradhan, “Fault-Tolerant Computer System Design,” Prentice Hall, UK, ISBN: 978-0130578877, 1996.
7. R. W. Butler and S. C. Johnson, “Techniques for Modeling the Reliability of Fault Tolerant Systems with the Markov State Space Approach,” Langley Research Centre, NASA Reference Publication 1348, Hampton, Virginia, USA, 1995.

8. S. Poledna, “Fault Tolerance and Modeling,” TU Wein University, URL: http://www.vmars.tuwien.ac.at/courses/ ftol/slides/FTS-VO-P3.pdf, 2004.
9. C. M. Greinstead and L. Snel, “Introduction to Probability,” An e-book from American Mathematical Society, URL: www.dartouth.edu/~chance/teaching_aids/book_articles/probability_book/chapter11.pdf , 2010.
10. E. Dubrova, “Fault Tolerant Design: An Introduction,” Kluwer Academic Publisher, 2008.
11. J. Bukowski and M. William, “Using Markov Models for Safety Analysis of Programmable Electronic Systems,” ELSEVIER ISA Transactions 34, pp.193-198, 1995.

7/31/2013