Safety and reliability assessment using fuzzy theory applied to a subway system

P.S. Cugnasca

Department of Computer Engineering and Digital Systems,
Polytechnic School, University of São Paulo, Brazil.

Abstract

For the last two decades the GAS – Safety Analysis Group - has been working on safety analysis of train and subway systems in order to certify the safety project of some private companies. Particularly, the subway of São Paulo City, Brazil, which has three lines and benefits a population of 18 million people of the Great São Paulo, is subject to a continuous analysis as the number of new lines is rapidly increasing.

The use of redundant architectures is one way of attributing higher safety and reliability to this kind of critical system. Several mathematical models have been used to aid in the safety and reliability assessment of safety-critical systems. Among these consecrated models are the combinatory model and the Markov model. These models depend on some parameters, such as fail rate and coverage factor, defined by component manufacturers or estimated by experts.

On the other hand, fuzzy theory plays an important role within the artificial intelligence area because of its mathematical modeling facility of vague concepts in the human language and imprecise data. That is related with the problem found by the system designers that sometimes do not have precise information to be used in the system safety and reliability evaluations. This paper presents a safety and reliability assessment aid tool of fault tolerant systems composed of redundant modules using fuzzy theory.

1 Introduction

In critical system applications, the incorrect performance of the system will almost certainly yield undesirable or disastrous results [1]. Particularly, in mass system transportation, thousands or millions people life could be put under risk situation when the control system fails or works improperly. Some aspects must
be considered when a critical system is being projected or analyzed: reliability, safety, availability, maintainability and others issues of importance [2]. The safety aspect is important because human life could be preserved if something goes wrong during the subway working. And also, the reliability and availability aspects, although could not be directly related with the safety component, they can give comfort and satisfaction to the final user.

Many times in the project analysis of a critical system the engineer is under a undesired situation: the lack of precise data about the reliability of individual components of the system. For instance, the reliability of a component or module of a system may be expressed by a range of values in a manufacturer databook, estimated by an expert system designer or obtained by any type of evaluation. In this case, the system reliability or safety assessment will result in a range of values.

This paper focuses on an alternative approach of deal with uncertainty, applied to redundant architectures, where the parameters present in reliability and safety models could not be precisely defined. As a result, the fuzzy theory will be applied in the Markov Model, which is used to reliability and safety assessment. This method allows a mathematical treatment of parameters not precisely defined (or defined with some degree of uncertainty) and provides reliability and safety curves with associated degree of confidence as well. This model incorporates the parameters failure rate, coverage factor and repair rate and permits the approximated reliability/safety assessment of a fault-tolerant system.

2 Fuzzy theory

One of Lotfi A. Zadeh’s first papers, “Fuzzy Sets” [3], gave a higher importance to the fuzzy theory in scientific environment in 1965. In that time, he formalized the basic concepts of fuzzy sets theory, which can be viewed as an extension of classical sets theory. Zadeh realized that some classes of objects do not admit the classical treatment of the conventional set theory and, as a consequence, the fuzzy theory could become a useful tool for modeling human activities with vague or imprecise information associated.

In this context, the fuzzy theory supplies a mechanism to deal with imprecise information [4] [5] [6]. Some researches describing the application of fuzzy theory in the reliability assessment of critical systems can be found in the specialized literature based on the combinatorial model [7] [8] [9] as well as the application of fuzzy logic in the risk analysis area [7].

In the classical sets (generally accepted in the literature as crisp sets) theory, to indicate that an individual object $x$ is a member of a set $A$, within a given universal set $X$, it is written:

$$x \in A.$$ (1)

Whenever $x$ is not an element of a set $A$, it is written:

$$x \notin A.$$ (2)

The characteristic function of a crisp set assigns a value either 1 or 0 to each element $x$ of $A$ in the universal set $X$, discriminating between members and
nonmembers of the crisp set. As fuzzy sets are an extension of crisp sets, this function can be generalized so that membership values assigned to elements of the universal set \( X \) fall within a continuous range of real numbers in the interval \([0, 1]\). Such function is called a membership function. Fuzzy sets will be represented with the character "~" associated in order to distinguish them from crisp sets. Thus, a general fuzzy set will be written in the form \( \tilde{A} \) and its membership function denoted by \( \mu_{\tilde{A}}(x) \) [10], as shown in Figure 1.

![Figure 1: Membership function.](image)

### 2.1 Basic concepts

The \( \alpha \)-cut of a fuzzy set \( \tilde{A} \) is the crisp set \( \tilde{A}_{\alpha} \) that contains all the elements of the universal set \( X \) whose membership degrees in \( \tilde{A} \) are greater or equal to a given value of \( \alpha \) \([0,1]\) (see Figure 1). Thus, given a fuzzy set \( \tilde{A} \) of elements in the universal set \( X \) and a number \( \alpha \in [0,1] \), the \( \alpha \)-cut can be written as follows:

\[
\tilde{A}_{\alpha} = \{ x \mid \mu_{\tilde{A}}(x) \geq \alpha \} .
\]  

The support of a fuzzy set \( \tilde{A} \) is defined as a crisp set obtained by the application of a \( \alpha \)-cut with \( \alpha \geq 0 \). A particular type of fuzzy set occurs when a single point defines the set; in this case, the fuzzy set is called fuzzy singleton. A fuzzy set \( \tilde{A} \) is called normal when the largest membership degree obtained by any element in the set is equal to 1 (see Figure 1).

### 2.2 Fuzzy numbers

Fuzzy numbers are fuzzy sets defined on the set \( \mathbb{R} \) of real numbers and represent the intuitive concept of approximate numbers, such as "numbers close to a given real number". A fuzzy set \( \tilde{A} \) defined on \( \mathbb{R} \), qualified as a fuzzy number, must possess at least the following properties [10]:

- \( \tilde{A} \) must be a normal fuzzy set;
- The support for \( \tilde{A} \) must be bounded; and
- \( \tilde{A}_{\alpha} \) must be a closed interval for every \( \alpha \in (0,1] \).
2.3 Fuzzy arithmetic

Fuzzy arithmetic is composed of arithmetic operations on fuzzy numbers. Two properties of fuzzy numbers are essential for fuzzy arithmetic [10]:

- Fuzzy numbers can fully be represented by their $\alpha$-cuts; and
- The $\alpha$-cuts of fuzzy number are closed intervals of real numbers for all $\alpha \in (0,1]$.

As a result, arithmetic on fuzzy numbers can be defined in terms of arithmetic operations on their $\alpha$-cuts or, in other words, in terms of arithmetic operations on closed intervals, which is supported by the classical mathematics. Now, the four arithmetic operations: addition ("+"), subtraction ("-"), multiplication ("\cdot") and division ("/"") will be generically denoted by the character "*". Thus, any operation between two elements $f$ e.g., belonging to intervals $[a,b]$ and $[c,d]$, respectively, can be written as

$$[a,b] * [c,d] = \{ f*g | a \leq f \leq b, c \leq g \leq d \}$$

except that $[a,b]/[c,d]$ is not defined when $0 \in [c,d]$. Consequently, the result of an arithmetic operation on closed intervals is also a closed interval. For instance, the addition, subtraction and multiplication operations on closed intervals are defined as follows [7] [10]:

$$[a,b] + [c,d] = [a+c, b+d] \tag{5}$$

$$[a,b] - [c,d] = [a-d, b-c] \quad \text{and} \tag{6}$$

$$[a,b] \cdot [c,d] = [\min(ac,ad,bc,bd), \max(ac,ad,bc,bd)] \tag{7}$$

Particularly, any real number $r$ may also be regarded as a special interval $[r,r]$. When one of the intervals is in this form (degenerated), the arithmetic operations are simplified; and, when both of them are degenerated, the result is a standard arithmetic operation of real numbers.

3 A generalized Markov model

Among the analytical system reliability models, the combinatorial modeling and the Markov modeling are the two most commonly used approaches. The combinatorial model enumerates the different ways in which a system can remain operational using probabilistic techniques. It is a useful method when the systems are simple and the coverage factor and the repair rates (corrective and preventive) are not considered. Otherwise, the Markov model is more suitable [1][11].

Several Markov model approaches are described in the literature: without coverage and without repair, including coverage and including repair [1][11]. Now, a generalized system with coverage factor, corrective repair rate and preventive repair rate is described, proposed in [12].

Let us consider the Markov model of a triple-modular redundancy (TMR) system with three identical modules in a voting arrangement, shown in Figure 2.
Each module has a constant failure rate $\lambda$ (obeying the exponential failure law [1]), a coverage factor $C$ (probability of detecting a fault), a corrective repair rate $\mu_c$ and a preventive repair rate $\mu_p$. The definition of the faulty and fault-free states will depend on the considered voting type (majority for safety applications and non-majority for high reliable applications). The state diagram resultant for this TMR system is schematically shown in Figure 3.

Figure 3: Transition diagram.

Generically, each state is represented as $S_{i,a}$, where $i$ is the number of fault-free modules and $a$ is the number of faulty modules without coverage. The system begins in state $S_{3,0}$, without faulty modules. In a given instant of time $t$, the system is in a generic state $S_{i,a}$, where the following events may occur within the time period $\Delta t$: module fault with coverage (right transition), module fault without coverage (right-down transition), corrective repair of a module (left transition) or preventive repair of a module (left-up transition). Upon a module failure, the system transits to a more failure representative state (with probability $i\lambda \Delta t C$, if the fault is detected, or $i\lambda \Delta t (1-C)$, if the fault is not detected). A repair may lead the system to a less failure representative state (with probability $a \mu_c \Delta t$, if a preventive repair corrects a not detected fault, or $(3-i-a)\mu_p \Delta t$, if a corrective
repair corrects a detected fault). Figure 4 shows the probability transition from a generic state to its neighbor states.

\[
\begin{align*}
(i+1)_{a-1} & \quad (i+1)\lambda \Delta t(1-C) \\
(a)\mu_p \Delta t & \quad 1-(i)\lambda \Delta t-(n-i-a)\mu_C \Delta t-(a)\mu_p \Delta t \\
(i+1)_{a} & \quad (i+1)\lambda \Delta t C \\
(n-i-a)\mu_C \Delta t & \quad (n-i+1-a)\mu_C \Delta t \\
i_a & \quad (i)\lambda \Delta t C \\
(i-1)_{a} & \quad (i)\lambda \Delta t (1-C) \\
(a+1)\mu_p \Delta t & \quad (i-1)_{a+1}
\end{align*}
\]

Figure 4: Probability transition.

For small values of \(\Delta t\), it is reasonable to consider that at most one event occurs during this period. All possible transitions and their associated probabilities are also shown in Figure 4.

The equations of the Markov model of the TMR system can be written in matrix form, which provides the probabilities of the system being in any generic state \(S_{ia}\). So,

\[
P(t+\Delta t) = A \cdot P(t) \tag{8}
\]

where \(P(t)\) is the probability state vector at time \(t\), \(P(t+\Delta t)\) is the probability state vector at time \(t+\Delta t\), and \(A\) is the transition matrix.

For an \(N\)-modular redundancy (NMR) system with \(n\) identical modules, in a given state \(S_{ia}\), the following considerations are true:

- there are \((i)\) fault-free modules;
- there are \((n-i)\) faulty modules;
- there are \((a)\) faulty modules without coverage;
- there are \((n-i-a)\) faulty modules with coverage; and
- \((i+a) \leq n\).

Then, for any generic state \(S_{ia}\) of the system, the probability of being in this state at time \(t+\Delta t\) yields:
A fuzzy reliability Markov model

This fuzzy approach is a superset of the classical Markov model, because it allows uncertainty-based parameters in the mathematical reliability evaluation. These parameters incorporate all the uncertainty about their values and are modeled as fuzzy numbers. The model may be used to the reliability evaluation of any redundant control/supervision system with identical modules whose outputs are the inputs of a voter. In order to simplify the presentation of this model (Fuzzy Markov Model), a non-redundant system with only one module with coverage factor will be considered, as shown in Figure 5.

The system begins in state $I_0$, without faulty modules. Upon a module failure with coverage, the system transits to state $0_0$ and a corrective repair may lead it again to the fault-free state; otherwise, if the failure is without coverage, the transition to state $0_1$ takes place and only a preventive repair can make the system return to state $I_0$. A state diagram showing possible states and state transitions is also shown in Figure 5.

![State diagram for a non-redundant simple system with coverage and repair.](image)

4 A fuzzy reliability Markov model

Furthermore, it should be observed that these considerations may be generalized to an NMR system, with $n$ identical modules, using the Generalized Markov Model previously presented. For this system, the equations of the Markov model can be written easily from the state diagram shown in Figure 4, in a matrix form. So,

$$P(t + \Delta t) = A \cdot P(t),$$

where

$$p_i(t + \Delta t) = \left[1 - (i + 1)\lambda\Delta t - (n - i - a)\mu_c\Delta t - (a)\mu_p\Delta t\right] p_{i-1} + \left[(i + 1)\lambda\Delta t(1 - C)\right] p_{i+1} \quad \text{for } (i + a) < n$$

$$+ \left[(i + 1)\lambda\Delta t\right] p_{i+1} \quad \text{for } a > 0$$

$$+ \left[(n - i + 1 - a)\mu_c\Delta t\right] p_{i-1} \quad \text{for } i > 0$$

$$+ \left[(a + 1)\mu_p\Delta t\right] p_{i+1} \quad \text{for } i > 0.$$
\[
\begin{align*}
P(t + \Delta t) &= \begin{bmatrix} p_{0_0}(t + \Delta t) \\ p_{0_1}(t + \Delta t) \\ p_{0_2}(t + \Delta t) \end{bmatrix}, \\
P(t) &= \begin{bmatrix} p_{0_0}(t) \\ p_{0_1}(t) \\ p_{0_2}(t) \end{bmatrix}, \\
A &= \begin{bmatrix} 1 - \mu_C \Delta t & 0 & \lambda \Delta t C \\ 0 & 1 - \mu_P \Delta t & \lambda \Delta t (1 - C) \\ \mu_C \Delta t & \mu_P \Delta t & 1 - \lambda \Delta t \end{bmatrix}.
\end{align*}
\] (11)

Assuming some initial value of the probability state vector \( P(0) \) (\( p_{0_0}(0) = 1, \\
p_{0_1}(0) = p_{0_2}(0) = 0 \)), the value of \( P(n \Delta t) \) can be obtained as:

\[
P(n \Delta t) = A^n \cdot P(0).
\] (12)

The Markov model parameters (\( \lambda, C, \mu_C \) and \( \mu_P \)) will now be modeled as fuzzy numbers in order to incorporate all the uncertainty related to their values. This way, as designers and analysts know the system and its constituent modules well, they are able to choose the best function that approximate their knowledge on these parameters. Then, these new fuzzy parameters will be represented as \( \tilde{\lambda} \), \( \tilde{C} \), \( \tilde{\mu}_C \) and \( \tilde{\mu}_P \) and are exemplified in Figure 6, where they are modeled by triangular membership functions. For instance, \( \lambda_N, \lambda_I \) and \( \lambda_S \) are the nominal value (\( N \)), inferior limit (\( I \)) and superior limit (\( S \)), respectively, of the parameter \( \lambda \) modeled as a fuzzy number (\( \tilde{\lambda} \)).

![Figure 6: Fuzzy Markov model parameters modeling.](image)

Particularly, if one or more parameters have no uncertainty associated, they can be represented by fuzzy-singletons, which are crisp values. As transaction matrix \( A \) is composed of operations on fuzzy numbers in this approach, it will be denoted by \( \tilde{A} \). The same occurs with the vector \( P(n \Delta t) \), which will be denoted by \( \tilde{P}(n \Delta t) \). Consequently, the resultant equations in a matrix form is:

\[
\tilde{P}(n \Delta t) = \tilde{A}^n \cdot P(0).
\] (13)

Cell 3x3 of matrix \( \tilde{A} \) is presented in Figure 7(a) in order to illustrate the operations involved.

![Figure 7: Cell 3x3 of the (a) original matrix \( \tilde{A} \); (b) evaluated matrix \( \tilde{A} \).](image)
Applying the fuzzy arithmetic on closed intervals to simplify this transition matrix, it can be seen that two fuzzy operations are necessary: subtraction and multiplication of fuzzy numbers. It must be said that although the result of the addition or the subtraction operations on two triangular fuzzy number is another triangular fuzzy number, the result of the multiplication operation on two triangular fuzzy numbers is similar to a triangle, but with curved edges. On the other hand, it is a common practice to approximate multiplication results by triangular functions. Hence, the approximated resultant evaluated cell 3x3 of matrix $\tilde{A}$ is shown in Figure 7(b). Finally, the fuzzy system reliability in time $n.\Delta t$, for the example of the system considered, is:

$$\tilde{R}(n\Delta t) = \tilde{P}_{10}(n\Delta t),$$

(14)

where $\tilde{P}_{10}(n\Delta t)$ is obtained from $\tilde{P}(n\Delta t)$.

This time response yields several reliability curves, one for each $\alpha$-cut. For instance, considering three values for $\alpha$-cut (0.0, 0.5 and 1.0), the fuzzy reliability produced by this method could be similar to that shown in Figure 8(a), where there are five curves, each with a particular confidence degree. Finally, in a given instant of time $i.\Delta t$, the fuzzy reliability may be approximated by a triangle, as shown in Figure 8(b), where each value of reliability has a membership degree in which the analyst believe the system has ($R_f(i.\Delta t)$ and $R_s(i.\Delta t)$ define a range of reliability values, each with its membership degree).

![Figure 8](image.png)

Figure 8: (a) Reliability curves for three $\alpha$-cuts; (b) Fuzzy reliability in a given instant of time ($i.\Delta t$).

5 A fuzzy safety Markov model

The fuzzy safety Markov model is similar to the fuzzy reliability Markov model. The forms for choosing the safe states in the Markov model and the parameters involved in the transitions are the main difference. Let us consider a TMR system with a fail-safe majority voter, as shown in Figure 2. A failure occurring in a given module can be safe (which does not lead the system to an unsafe state) or unsafe (which does lead the system to an unsafe state). In this approach only the unsafe failures are important. Considering the exponential failure law, each module has a constant unsafe failure rate $\lambda_u$. 

© 2002 WIT Press, Ashurst Lodge, Southampton, SO40 7AA, UK. All rights reserved. 
Web: www.witpress.com Email witpress@witpress.com
6 Conclusion

The greatest benefit from the application of the Fuzzy Markov Model is to take advantage of the designer’s or analyst’s experience, specially when there are uncertainty-base values on the Markov model parameters. In this case, the lack of exact knowledge about one or more parameters values does not avoid obtaining system reliability or safety. As a result, this model yields reliability/safety curves that show the variation of the “fuzziness” degree of reliability/safety at each instant of time. Furthermore, these curves depend on the parameters imprecision adopted. As imprecision tends to zero, these curves approximate that obtained through the traditional Markov model. At this moment, this tool is being applied to the hardware analysis of the São Paulo subway system which has a triplicate hardware with a fail-safe voter, allowing an alternative way to estimate its reliability and safety.

References