Determining Safety Integrity Level by Considering Uncertainty Aspects in Fuzzy Environment (Case Study on Train Braking System)

Hasti Jafari¹, Mohammad Ali Sandizadeh¹*, Amir Ghavibazoo¹

¹School of Railway Engineering, Iran University of Science and Technology, Tehran, Iran

ARTICLE INFO

The industry sectors occasionally face the difficulty of safety level determination of safety systems. Some standards including ISAS 84.01 and IEC61508 have provided some guidelines but there is no a complete and comprehensive understanding about these standards and their accomplishment. It should be noted that the security analysis is one of the most important factors to measure the risk level, as its measurement in certain environment is difficult, so in this study a new approach is proposed to analyze the risk level of safety instruments in fuzzy environment. The new methodology is applied on a train braking system as a case study and the results indicated that the level of safety integrity level is influenced by the security factors. The determination of safety integrity level needs to implement the safety functions and the uncertainty of probabilistic model parameters, which are affected by the results of security analysis. The level of safety integrity in fuzzy environment is calculated by proposing fuzzy fault tree analysis and the results have been compared with the concluded results obtained from certain methods.

1. Introduction

The understanding and analyzing of intricate systems is an important issue because of the increased number of users. The happened industrial events in recent years have caused changes in experts' approach about the safety. In this regard, many widespread actions have been applied in recent years and many standards have been designed and formulated including the international standard IEC61508 and ISAS 84.01. Prior to these standards, there was not a comprehensive understanding of the way to determine the safety integrity level (SIL) of safety instrument systems (SIS) and the safety level of system could be determined by the reliability calculation of system failures. For example, we can note that Simpson and Gulland (in 2003) applied the Markov method in two separate studies to determine the level of safety integrity for the reparable safety systems and they stated that this methodology makes to achieve the wrong results [1]. In 2004, D. J. Smith and K. G. L. Simpson published their experience in the implementation of IEC61508 standard as a book [2]. Rouvroye and Wiegerinck noted that the periodic functional tests are incomplete and they implemented a new methodology for minimizing the cost of implementing the safety integrity level of the systems [3]. Also in another study in 2006, J. V. Bukowski attempted to determine the level of safety systems with exponential distribution of time repair [4]. In 2007, X. Yang and H. Guo attempted to analysis the level of safety systems by the usage of RBD methodology [5]. Beugin, Renaux and Cauffriez tried to measure the Safety level of systems by Considering the environmental changes of working conditions and Baybutt measured the safety level by optimizing the Risk graph [6] [7]. In another

*Corresponding author, Associate professor
Email: sandizadeh@iust.ac.ir
Determining Safety Integrity Level by Considering Uncertainty Aspects in Fuzzy Environment …

... the typical way of safety systems are shown in Fig 1. [17]. One of the layers presented in the figure is...
called safety Instrumented System (SIS) consisting of sensors, logical solver and final components to achieve safe situation by taking some process. SIL is defined as the safety function of the SIS, which can be found by its PFD [25].

3. SIL Analysis by the usage of the Fuzzy Fault Tree

In this method, these stages are the main process to reach the system failure rate:

- Analyzing the fault tree of safety system.
- Preparing function belongs to failure rate of each system component.
- Preparing the smallest non-repetitive discontinuity sets for the fault tree obtained.
- The calculation operations of fuzzy numbers to obtain the function of fault rate in the demand time.
- The determination of function belongs to each level of safety integrity.

3.1. Fuzzy Numbers

If a continuous variable $x$ belongs to $\mu_0 \in [0,1]$, satisfying the following assumptions, can be considered as a fuzzy number.

- $\mu_0$ is a continuous set of variables;
- $\mu_{c0}$ is a convex fuzzy set;
- $\mu_{n0}$ is a normal fuzzy set.

To reduce the computational operation the membership functions is defined in $\alpha$ level.

The membership function of a fuzzy number $A$ is shown by $\mu_A(x)$ and two points are used to demonstrate the interval bounded of this value at $\alpha$ level ($0 \leq \alpha \leq 1$) by the usage of $\alpha$ cut method. The lower and the upper bounds of this interval are shown by $A_{\alpha L}$ and $A_{\alpha U}$ respectively [11].

3.2. Fuzzy Fault Tree Analysis

Each event has a degree of uncertainty and the probability of top event can be calculated by the probabilities of each component failures. A simple calculation of fuzzy fault tree analysis is shown in Fig 3.

It is assumed that each event is independent and the top event failure rate can be calculated by:

$$P_{(o)} = \sup\{PA_1+PA_2\min\{PA_1,PA_2\}\} \tag{1}$$

4. Case Study

In this section, we test our model by using an example of JI Simpson study (2004) [2] on braking system of trains.
In mentioned system, there are two safety systems. We combine the primary and emergency braking systems. The first one is a system with high demand and the other one is a low demand system.

Initial studies showed that this set braking system covers third level of safety integrity. These two braking systems are dependent, so, we could consider the braking system as an integrity set or have two separate systems and SIL can be calculated by multiplying two fault rates. The ‘high demand’ system activated not only by the train driver but also by receiving the automatic signal to send electronic signals and consequently the brake pressure can be transferred to each bogie by the usage of an air valve.

The air generator can supply the air pressure for each bogie to operate the brakes. The braking will be reduced by %25 if one bogie braking system is broken. When three out of the four bogies are operated, the safety function can be considered in a good condition. Regarding to mentions above, we attempt to model the system fault tree. There are some assumptions that are considered in the paper such as: The time distribution is considered constant for the fault rates of components. It is assumed that the design faults (Bum-in failure), Wear out-failure and Preventive – failure have been removed. Common cause failure of parallel systems determined by the beta factor and the beta value is considered 1%. For SIL quantitative analysis, knowing the fault rate of subset components is essential. The fault rates determined by JL Simpson [2] are shown in Table 2.
Table 2. Failure rates of braking system component [3]

<table>
<thead>
<tr>
<th>Subsystem name</th>
<th>Failure mode</th>
<th>Failure rate of subsystem (overall) (10^-6 per hour)</th>
<th>Failure rate of Subsystem (failure mode) (10^-6 per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE control of cabin</td>
<td>The output serial is low</td>
<td>2</td>
<td>0.6</td>
</tr>
<tr>
<td>PE control of bogie</td>
<td>The output analogue is low</td>
<td>2</td>
<td>0.6</td>
</tr>
<tr>
<td>Air control valve of primary brake</td>
<td>Unable to move</td>
<td>5</td>
<td>1.5</td>
</tr>
<tr>
<td>Solenoid valve</td>
<td>Unable to open</td>
<td>0.8</td>
<td>0.16</td>
</tr>
<tr>
<td>Initial brake lever</td>
<td>Does not work</td>
<td>1</td>
<td>0.1</td>
</tr>
<tr>
<td>Emergency brake lever</td>
<td>Not disrupt the flow of electricity</td>
<td>1</td>
<td>0.1</td>
</tr>
<tr>
<td>Bogie air reservoir</td>
<td>Fail</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Brake shoes</td>
<td>Fail</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>Common errors of Wind Tanks</td>
<td></td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td>same reason of brake shoe failures</td>
<td></td>
<td>0.005</td>
<td></td>
</tr>
</tbody>
</table>

4.1. Primary braking analysis by the fuzzy fault tree

The analysis of primary braking system is shown in Fig 5, which gates G22 and G23 are similar to G21 and G24 so are not shown in the figure.

Fault rate obtained from J.L. Simpson fault analysis is calculated 0.550E-07, so this system is third level of safety integrity. Here by comparison the study in fuzzy environment, the fault tree can be found. We assume that fault rate has the interval between 5% and 10%. This fault rates are shown in Table 3.

Table 3. Fault rate of system components reliability

<table>
<thead>
<tr>
<th>Component names</th>
<th>Maximum fault rate</th>
<th>average fault rate(m)</th>
<th>Minimum fault rate(LL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCFB</td>
<td>5.E-04</td>
<td>5.E-04</td>
<td>5.E-04</td>
</tr>
<tr>
<td>EMERG</td>
<td>1.E-02</td>
<td>1.E-02</td>
<td>9.E-03</td>
</tr>
<tr>
<td>PE1</td>
<td>6.E-02</td>
<td>6.E-02</td>
<td>5.E-02</td>
</tr>
<tr>
<td>LEVER</td>
<td>1.E-02</td>
<td>1.E-02</td>
<td>9.E-03</td>
</tr>
<tr>
<td>CCFA</td>
<td>5.E-03</td>
<td>5.E-03</td>
<td>5.E-03</td>
</tr>
<tr>
<td>AIR21</td>
<td>1.E-01</td>
<td>1.E-01</td>
<td>9.E-02</td>
</tr>
<tr>
<td>BRAK21</td>
<td>5.E-02</td>
<td>5.E-02</td>
<td>5.E-02</td>
</tr>
<tr>
<td>SOL21</td>
<td>2.E-02</td>
<td>2.E-02</td>
<td>1.E-02</td>
</tr>
<tr>
<td>VAL21</td>
<td>2.E-01</td>
<td>2.E-01</td>
<td>1.E-01</td>
</tr>
<tr>
<td>AIR22</td>
<td>1.E-01</td>
<td>1.E-01</td>
<td>9.E-02</td>
</tr>
<tr>
<td>BRAK22</td>
<td>5.E-02</td>
<td>5.E-02</td>
<td>5.E-02</td>
</tr>
<tr>
<td>SOL22</td>
<td>2.E-02</td>
<td>2.E-02</td>
<td>1.E-02</td>
</tr>
<tr>
<td>PE22</td>
<td>6.E-02</td>
<td>6.E-02</td>
<td>5.E-02</td>
</tr>
<tr>
<td>VAL22</td>
<td>2.E-01</td>
<td>2.E-01</td>
<td>1.E-01</td>
</tr>
<tr>
<td>AIR23</td>
<td>1.E-01</td>
<td>1.E-01</td>
<td>9.E-02</td>
</tr>
<tr>
<td>BRAK23</td>
<td>5.E-02</td>
<td>5.E-02</td>
<td>5.E-02</td>
</tr>
<tr>
<td>SOL23</td>
<td>2.E-02</td>
<td>2.E-02</td>
<td>1.E-02</td>
</tr>
<tr>
<td>VAL23</td>
<td>2.E-01</td>
<td>2.E-01</td>
<td>1.E-01</td>
</tr>
<tr>
<td>AIR24</td>
<td>1.E-01</td>
<td>1.E-01</td>
<td>9.E-02</td>
</tr>
<tr>
<td>BRAK24</td>
<td>5.E-02</td>
<td>5.E-02</td>
<td>5.E-02</td>
</tr>
<tr>
<td>SOL24</td>
<td>2.E-02</td>
<td>2.E-02</td>
<td>1.E-02</td>
</tr>
<tr>
<td>VAL24</td>
<td>2.E-01</td>
<td>2.E-01</td>
<td>1.E-01</td>
</tr>
</tbody>
</table>
4.2. Determination the Alpha cut for each basic event

To calculate the alpha cut we used this formula

\[
u_a(x) = \begin{cases} 
\frac{(x-LL)}{(m_{-LL})}, & LL \leq x < m \\
\frac{(UL-x)}{(m_{UL})}, & m \leq x \leq UL \\
0, & x > UL, x < LL 
\end{cases}
\]

(2)

The Alpha cut for each basic event is shown in Table 4.

In this section, the basic events and alpha cuts have been shown in the Table 5.

We calculate the probability of top event (TE), and the alpha cut is shown here:

\[
P(TE)_a = 5 \times 10^{-8} + 6 \times 10^{-6} \alpha + 7 \times 10^{-10} \alpha^2
\]

\[
P(TE)_a' = 5 \times 10^{-8} + 6 \times 10^{-6} \alpha + 7 \times 10^{-10} \alpha^2
\]

(3)

\( \alpha \in [0,1] \)

Since the coefficients of the third and the fourth grades are suppressed because these are small. The alpha cut for the top event is shown here:
The fault rate diagram of top event by considering different values of alpha is shown in Figure 6.
By comparison the lower and the upper bounds of fault rate of system top event with the different levels of safety integrity table, we can understand that the system has the third level of safety integrity of high demand systems.

6. Conclusions

In this paper, we try to show the importance of safety analysis and to express the safety integrity level in the fuzzy environment. Finally, its application is shown in the train braking system to determine the SIL of this system. The procedure in this case study is proposed as a methodology for the SIL quantitative measurement by considering the uncertainty in the model parameters.

References