Safety Analysis of Level Crossing Surveillance Systems Using Fuzzy Petri Nets

Chi-Chung Tao Tsung-Chin Lin
Tamkang University
cctao@mail.tku.edu.tw

Abstract

A backward safety analysis model that can deal with dangerous status by virtue of fuzzy theory is proposed in this paper. Fuzzy Petri Nets (FPN) is developed and applied to the safety analysis for three types of level crossing surveillance systems of Taiwan Railway Administration. The numerical results of proposed FPN models are fairly plausible.

1. Introduction

Complex component-based systems used in mission- or safety-critical domains, including defense applications, air traffic control, railway signaling and medical applications play an important role in our modern society. One important task in the development of these systems is the construction of safe cases and risk assessment models that are used to determine quantitative measures for failure or hazard probabilities. These safety analysis models should be intuitive, compositional and have the expressive power to model both software and hardware behavior [1]. In industrial projects, currently event-based models such as Fault Trees or state-based models such as Markov chains are used. Each of these models has it limitations [2]. State Event Fault Trees (SEFTs) are a hierarchical and visual model that integrates elements from stochastic state-based models (Markov-chains) with Fault Trees [3]. A model that combines elements from Fault Trees and Markov Models was proposed to improve expressive power of safety cases [4].

Recently Petri nets have been used to model and analyze for such complex component-based systems regarding properties as safety and failure-tolerance [5, 6]. Many fairly good results of real case studies proved the advantages of Petri nets since hardware, software, and human behavior can be modeled using the same model. However, complex component-based systems themselves are required to handle fuzzy information for safety critical issues. It is strongly recommended that fuzziness must be taken into account for safety analysis. Combining with Petri net and knowledge representation, a Fuzzy Petri Nets (FPN) can be used to depict fuzzy generating rules that can be taken as rules of fuzzy relationships between two propositions.

Using the hazardous states and fuzzy information that have been identified in the preliminary stage, it may be possible to analyze backward to the system, that is, hardware, software, and human, using FPN and thus to derive safety requirements. In this paper, we propose a safety analysis method using a FPN model which can handle fuzzy information. The effectiveness of this method is demonstrated with a case of level crossing surveillance systems that are already in operation or will be installed in near future by Taiwan Railway Administration (TRA).

The structure of this paper is organized as follows. In section 2, we describe fundamental principles of FPN. Section 3 illustrates the safety models of three scenarios of level crossing surveillance systems, and numerical tests are conducted to calculate fuzzy numbers to validate the proposed approach. Finally, the conclusions are drawn in section 4.

2. Fundamental Principles

FPN expanded from a Petri net is a bidirectional graph that has place and transition nodes like the Petri net. However, in FPN a token incorporated with a place is associated with a real value between 0 and 1; a transition is associated with a certain factor (CF) between 0 and 1. At the same time enabling and firing rules of a transition are also updated. There are nine elements in the structural definition of FPN [7]. The definition is follows:

$$FPN = (P, T, F, I, O, D, \mu, \alpha, U) \quad (1)$$

where,

$P=\{p_1,p_2,\ldots,p_n\}$ is a finite set of places; corresponding to the propositions of fuzzy production rules;

$T=\{t_1,t_2,\ldots,t_m\}$ is a finite set of transitions, $P \cap T=\phi$; corresponding to the execution of fuzzy production

978-0-7695-3435-0/08 $25.00 © 2008 IEEE
DOI 10.1109/ICIII.2008.175

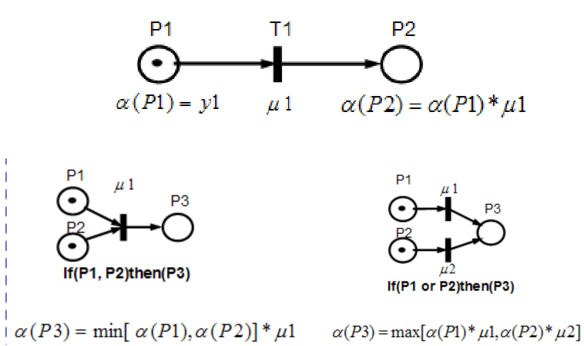
rules;
F is a set of directional arcs, $F \subseteq (P \times T) \cup (T \times P)$;
I: is the input incidence matrix and $I = \{\delta_{ij}\}$, where δ_{ij} is a logical value, $\delta_{ij} \in [0,1]$,$\delta_{ij} = 1$ when P_i is the input of T_j, otherwise, $\delta_{ij} = 0$, i=1,2,…,n, j=1,2,…,m;
O: is the output incidence matrix and $O=\{\gamma_{ij}\}$, where γ_{ij} is a logical value, $\gamma_{ij} \in [0,1]$, γ_i=1 when P_i is the output of T_j , otherwise γ_{ij}=0,i=1,2,…,n, j=1,2,…,m;
$D=\{d_1,d_2,\ldots,d_n\}$ is a finite set of propositions of fuzzy production rules. $|P|=|D|$; |.| denotes the number of its elements;
μ: $T \to [0,1]$ is the function which assigns a threshold μ_i between 0 and 1 to transition t_i;
α: $P \to [0,1]$ is the function which assigns the degree of truth between 0 and 1 to each place;
$U=U\{u_1,u_2,\ldots,u_m\}$, where u_i denotes the certainty factor (CF) of R_i, which indicates the reliability of the rule R_i, and $u_m \in [0,1]$.

Knowledge rules of FPN are summarized as follows:
$R1$: IF d_i THEN $d_j \Rightarrow$ (CF=u_i) $\Rightarrow d_i \to dj$
$R2$: IF d_i AND d_j THEN $d_k \Rightarrow$ (CF= u_i) $\Rightarrow d_i \cap d_j \to d_k$
$R3$: IF d_i OR d_j THEN $d_j \Rightarrow$ (CF=u_i) $\Rightarrow d_i \cup d_j \to d_k$

In these rules, di and dj represent precondition set, d_k represents an action or conclusion. $u_i \in [0,1]$ is a CF of a rule.

During fuzzy inferring and, we should establish three sets (RS, IRS, AP) for each place. For a specific place p_i:
$RS(p_i)$: a reachable place set of p_i, no matter how many transitions are fired.
$IRS(p_i)$: a place set that p_i can reach through one transition.
$AP(p_i)$: all the places that through one transition can reach the place that p_i can reach through one transaction.

In order to enhance inferring efficiency, backward inference mechanism shown in Fig. 1 is used.



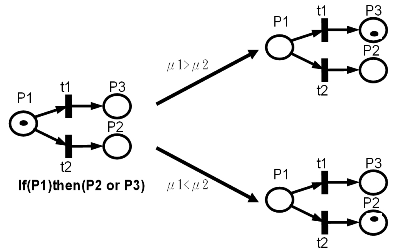


Figure 1. Backward fuzzy inference mechanism

3. FPN Models of Level Crossing Surveillance Systems

The existing level crossing surveillance system of TRA is based on infrared detection technology. It is now in progress that a video image processing-based surveillance system will be installed at several level crossings. TRA has, therefore, three types of level crossing surveillance systems in the future, i.e. the infrared, the video image processing and both of them (hybrid one). Three Petri nets models are hence constructed for these level crossing surveillance systems. An example of Petri nets model of the hybrid system combining the infrared and the video image processing technologies is shown in Fig. 2. The states of place and transition for this hybrid system can be summarized in Table 1.

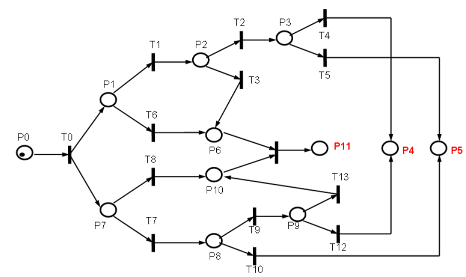


Figure 2. Fuzzy petri nets of the hybrid system

Table 1. States of place and transition of the hybrid system

State of place	Description	State of transition	Description
P_0	Receive radio commands	T_0	Transmit starting commands
P_1	Start video image surveillance	T_1	System is normal
P_2	Transmit video images	T_2	Video images are recognizable
P_3	Receive messages from the train	T_3	Video images are not recognizable
P_4	Train Stops	T_4	Train can not pass
P_5	Train passes	T_5	Train can pass
P_6	Video image surveillance fails	T_6	System is abnormal
P_7	Start infrared surveillance	T_7	System is abnormal
P_8	Send infrared signals	T_8	System is normal
P_9	Transmit train stop signals	T_9	Incident occurs
P_{10}	Infrared surveillance fails	T_{10}	No incident
P_{11}	Dangerous status	T_{11}	Protection system fails
		T_{12}	Signals are receivable
		T_{13}	Signals are not receivable

The fuzzy analysis of the hybrid system which is the standard type 3A of TRA's level crossing surveillance system can be performed by defining fuzzy functions and fuzzy rules.

3.1. Fuzzy functions

The relative situations of Petri nets conflicts in this paper are: "system is normal or abnormal", "video images are recognizable or not recognizable", "incident occurs or not occur", "signals are received or not received" and "train can pass or not pass". The paired fuzzy functions are defined with common indexes shown in table 2.

Table 2. Fuzzy functions and indexes

Function	Index
System is normal or abnormal	Time
Video images are recognizable or not recognizable	Transmitting intervals of video images
Incident occurs or not occur	Seconds of infrared interrupts
Signals are receivable or not receivable	Ratio of signal noise
Train can pass or not pass	Distance from level crossing gate

The upper limit values of fuzzy index for video image processing surveillance system and infrared surveillance system are set as 2.2401 K-hours and 1.464 K-hours, respectively (shown in Fig. 3 and Fig.4).

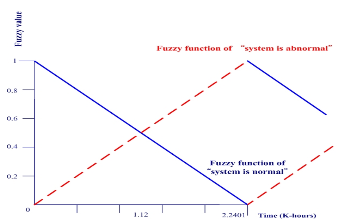


Figure 3. Fuzzy function of video image system

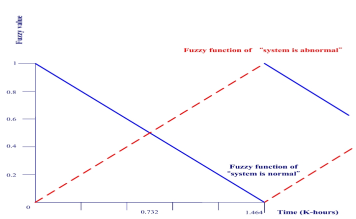


Figure 4. Fuzzy function of infrared system

The warning time of a level crossing device till the train arrives is at least 30 seconds based on TRA's operation rules. The upper limit value of fuzzy index for video recognition is hence set as 30 seconds (shown in Fig. 5). As to the time to detect incident whether occurs or not, it needs at least 2 seconds for infrared surveillance system to identify. The upper limit value of fuzzy index for infrared interrupts is set as 2 seconds (shown in Fig. 6).

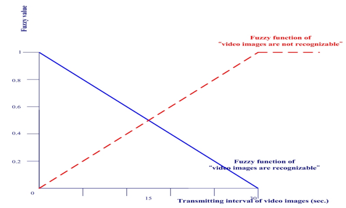


Figure 5. Fuzzy function of video image recognition

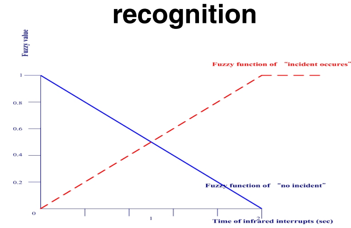


Figure 6. Fuzzy function of incident occurring

The upper limit value of fuzzy index for signal receiving is represented by ration of signal noise in percentage (shown in Fig. 7). When train driver receives signals to stop the train, the distance from level crossing gate for car approaching is set as 21.6 meters according to TRA's 3A type level crossing manual (shown in Fig. 8).

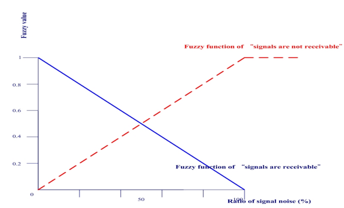


Figure 7. Fuzzy function of Signal receiving

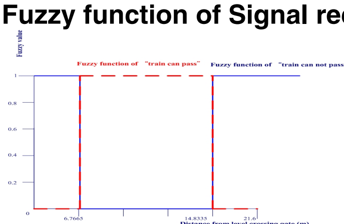


Figure 8. Fuzzy function of train passing

3.2. Fuzzy rules

The fuzzy rules for Petri nets model of Fig.2 are summarized in Table 3.

Table 3. Fuzzy functions and indexes

Rule	Description
R1	if (P_0) then (P_1 and P_7)
R2	if (P_1) then (P_2 or P_6) $\Rightarrow \mu_6 \geq \mu_1 \rightarrow T_6$, $\mu_6 < \mu_1 \rightarrow T_1$
R3	if (P_2) then (P_3 or P_6) $\Rightarrow \mu_3 \geq \mu_2 \rightarrow T_3$, $\mu_3 < \mu_2 \rightarrow T_2$
R4	if (P_3) then (P_4 or P_5) $\Rightarrow \mu_4 \geq \mu_5 \rightarrow T_4$, $\mu_4 < \mu_5 \rightarrow T_5$
R5	if (P_7) then (P_8 or P_{10}) $\Rightarrow \mu_8 \geq \mu_7 \rightarrow T_8$, $\mu_8 < \mu_7 \rightarrow T_7$
R6	if (P_8) then (P_9 or P_5) $\Rightarrow \mu_9 \geq \mu_{10} \rightarrow T_9$, $\mu_9 < \mu_{10} \rightarrow T_{10}$
R7	if (P_8 and P_3) then (P_5) $\Rightarrow \mu_9 < \mu_{10}$ and $\mu_4 < \mu_5 \rightarrow T_{10}$
R8	if (P_9) then (P_{10} or P_4) $\Rightarrow \mu_{13} \geq \mu_{12} \rightarrow T_{13}$, $\mu_{13} < \mu_{12} \rightarrow T_{12}$
R9	if (P_9 and P_3) then (P_4) $\Rightarrow \mu_{13} < \mu_{12}$ and $\mu_4 \geq \mu_5 \rightarrow T_{12}$
R10	if (P_6 and P_{10}) then (P_{11})

The rules above are based on single condition, multiple conditions of fuzzy inferences are therefore not necessary to be discussed here.

4. Numerical Tests

Based on fuzzy rules above, the fuzzy values of final states for three FPN models are computed according to various scenarios if the input value $\alpha(P_0)$ =1. For instance, the fuzzy values are 0.64287 and 0.54644, respectively when video image surveillance system is normal while infrared surveillance system is abnormal under the condition of 0.8 K-hours. Table 3 shows the input values of fuzzy functions under various scenarios.

Table 3. Input values of fuzzy functions under various scenarios

Scenario	Time (K-hours)	Transmitting interval of video images (sec)	Distance from level crossing gate (m)	Time of infrared interrupts (sec)	Ratio of signal noise (%)
A	0.6	14	6	0.5	–
B	0.6	14	10	1.5	45
C	0.6	14	10	0.5	–
D	0.6	14	6	1.5	45
E	0.8	14	6	–	–
F	0.8	14	10	–	–
G	2	–	–	0.5	–
H	2	–	–	1.5	45
I	1.2	–	–	–	–
J	0.6	16	–	1.5	55
K	0.8	16	–	–	–
L	2	–	–	1.5	55

The computed fuzzy values of final states of FPN models for "train can pass", "train stops" and "dangerous status" under various scenarios are summarized in Table 4.

Table 4. Numerical results of various scenarios

Scenario	Video image processing			Infrared			Hybrid system		
	Train can pass	Train stops	Dangerous status	Train can pass	Train stops	Dangerous status	Train can pass	Train stops	Dangerous status
A	0.39048	0	0	0.44262	0	0	0.44262	0	0
B	0	0.39048	0	0	0.24344	0	0	0.39048	0
C	0	0.39048	0	0.44262	0	0	0	0.39048	0
D	0.39048	0	0	0	0.24344	0	0.39048	0	0
E	0.34286	0	0	0	0	0.54644	0.34286	0	0
F	0	0.34286	0	0	0	0.54644	0	0.34286	0
G	0	0	0.89281	0.47541	0	0	0.47541	0	0
H	0	0	0.89281	0	0.26147	0	0	0.26147	0
I	0	0	0.53569	0	0	0.81967	0	0	0.53569
J	0	0	0.39048	0	0	0.24344	0	0	0.24344
K	0	0	0.34286	0	0	0.54644	0	0	0.34286
L	0	0	0.89281	0	0	0.26147	0	0	0.26147

Except scenario A and H the infrared system performs better than the video image surveillance system in "train can pass" and "train stops", it is found that the final state of video image surveillance system significantly differs from the infrared system under most scenarios. A train driver can simply judge whether to stop the train with the help of video images which reliability is naturally higher than the infrared system.

5. Conclusions

The dangerous status of the hybrid level crossing surveillance system can be detected under following necessary condition:

$$\textbf{IF } \{\mu_6 > \mu_1 \textbf{ OR } \mu_3 > \mu_2\} \textbf{ AND } \{\mu_8 > \mu_7 \textbf{ OR } [\mu_9 > \mu_{10} \textbf{ AND } \mu_{13} > \mu_{12}]\}$$

In addition, the fuzzy values of final states of three FPN models are also computed under various scenarios to identify the safety or risk status of certain level crossing surveillance system by constructing customized fuzzy rules.

However, it is recommended that multiple rules of fuzzy inferences are taken into account and the thresholds of several fuzzy values should be also specified to enhance the reliability of presented FPN models. In the future we'll develop a model based on Fuzzy Colored Petri net (FCPN) which is expected to have more expressive power than other Fuzzy Petri nets.

References

[1] J. Braband and H. Peters, "Experience with Quantified Safety Analysis", *Signal+Draht*, April, Tetzlaff Verlag, Hamburg, 2003.

[2] A. Villemeur, *Reliability, Availability, Maintain-ability, and Safety Assessmen*, John Willey and Sons, ISBN: 0-47193-048-2, 2000.

[3] L. Grunske , B. Kaiser, Y. Papadopoulos, "Model-Driven Safety Evaluation with State-Event-Based Component Failure Annotations", *Eighth International SIGSOFT Symposium on Component-based Software Engineering (CBSE 2005) Co-Located with ICSE-2005*, St Luis, Missouri, May 14-15, 2005.

[4] C. C. Tao, "A Combinatorial Approach to Quantify Stochastic Failure of Complex Component-Based Systems-The Case of an Advanced Railway Level Crossing Surveillance System", *Proceedings of Fourth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2007)*,*Vol.4*, China, pp.301-306,2007.

[5] S. Collart-Dutilleul, F. Deffossez, P. Bon, "Safety Requirements and P-time Petri Nets: A Level Crossing Case Study," *IMACS-IEEE Multiconference on Computational Engineering in Systems Applications*, pp. 1118-1123, 2006.

[6] Q. Lu, G. Huang and H. Zhu, "Fuzzy Analysis of Accidents Diagnosis Based on Fuzzy Petri Nets", *International Journal of Systems Control*, *Vol. 2*, *No.3*, pp.228-236, 2007.

[7] J. Yuan, H. Shi, C. Liu and W. Shang, " Backward Concurrent Reasoning Based on Fuzzy Petri Nets", *Proceedings of World Congress on Computational Intelligence 2008*, Hong Kong, pp. 832-837, 2008.