Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 7 (2010) 81–87

Procedia Engineering

www.elsevier.com/locate/procedia

2010 Symposium on Security Detection and Information

Applying Bayesian Networks in Nuclear Power Plant Safety Analysis

Guobing Chen, Zichun Yang, Jihong Sun *

College of Naval Architecture and Power, Naval University of Engineering, Wuhan, China

Abstract

Over the last decade, Nuclear energy has become one of important energy. Nuclear power systems become more complex and traditional safety methods are hard to be applied. This paper presents a novel approach for nuclear power plant safety analysis which called Bayesian Networks(BN). The BN model is constructed based on the combination of Failure Mode, Effect Analysis (FMEA) and Fault Trees Analysis(FTA). The probability of the model's root nodes is estimated by Bayesian estimation method and Monte Carlo simulation. Bidirectional inference and sensitivity analysis of the model is also researched. At last, we use a case study to show the method's advantages compared with traditional methods in nuclear power plant safety analysis.

Keywords: Nuclear Power Safety, Bayesian Networks, Failure Mode Effect Analysis, Fault Trees Analysis

1. Introduction

The development and peaceful use of nuclear energy was one of the most outstanding achievements in the history of the 20th century. Nuclear energy had been considered a economical, safe, reliable, clean energy. Faced with economic, security, nonproliferation, and environmental challenges, many countries had cost plenty manpower and material resources to develop nuclear safety research. Although personal injury in nuclear power plant accident was the lowest in the industry, but the influence of the accident was enormous. Such as Three Mile Island nuclear accident, Chernobyl nuclear accident and so on. So it was important to analyze the nuclear power safety.

The main characteristics in nuclear power safety analysis were:

(1) Complicated structure. Nuclear power equipments not only had complicated structure, plenty of units, but also practiced as polymorphism, uncertainty, failure dependency[1],. With few numbers and lacking information in

* Corresponding author. Tel.: 1-347-622-3524.
E-mail address: chenguob@163.com.

1877-7058 © 2010 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2010.11.012

complex nuclear power systems, the traditional safety analysis methods were difficult to accurately assess their safety.

(2) Strict safety management. Nuclear power plant must be operated by strict safety management. So its safety analysis should include safety management, and provide foundation for safety decision-making.

(3) Human factors. Human factors were an important side in nuclear safety. So the new safety method should expediently deal with human factors.

FMEA and FTA were both the most important methods in system safety analysis. FMEA dealt with single point failure, was built bottom to up, and presented as tables. FTA analyzed combinations of failures, was built top to down, and presented as diagrams. Both FMEA and FTA had advantages and disadvantages. FMEA has been heavily dependent on personal experience and information, and can not deal with the combination of various failure and human factors. FTA may miss some failure modes. Large fault trees were not easy to understand and their mathematics were often non-unitary solution. For complex nuclear power systems safety analysis, FMEA and FTA had obvious shortcomings.

It was a useful way to integrate FMEA and FTA for safety analysis of complex nuclear power systems. Its combination not only combined their advantages of these two methods, but also addressed both deficiencies. Many people had studied the combination of FMEA and FTA (FMEA/FTA). Zigmund Bluvband[2]introduced Bouncing Failure Analysis(BFA), which connected the two methodologies allowing an analyst from FTA to FMEA and back, changing the presentation and the direction of the analysis for convenience of analysis at any point in the process. Robyn R. Lutz [3,4]proposed a bi-directional analysis to integrated extension of software FMEA(SFMEA) and software FTA(SFTA), and used the bi-directional analysis to solve the safety analysis of software with high reliability.

Although the FEMA/FTA addressed part of the shortcomings of FMEA and FTA, but it was still inadequate for complex nuclear power system, and can not solve the polymorphism, failure dependency and uncertainties. Bayesian Networks, which rapidly developed in recent years, was a powerful tool to process polymorphism, dependency and uncertainty for nuclear power system. Bayesian Networks (BN) was one of the important analysis techniques in information theory, system engineering and other fields. Bobbio and Portinale introduced BN to reliability analysis by mapping fault tree into BN[5]. Burton Lee carried out a detailed study in BN modeling and analysis based on FMEA in system design phase[6,7]. This paper proposed the BN method based on FMEA/FTA, and used Bayesian estimate, Monte Carlo simulation to assess the probability of root nodes. This method not only addressed FMEA/FTA own shortcomings, but also solved the difficulties in safety analysis of complex nuclear power system. This method combined the FMEA and FTA information, which consistent with Bayesian information theory and made the model more accurate.

2. Combination of FMEA and FTA(FMEA/FTA)

FMEA was a method to analyze the product's all possible failure models and possible impact of each failure mode, and classify the severity of impact and probability of each failure model[8].FMEA had been proposed since the 50 years of the 20th century, and widely used in aerospace industry, micro-electronics industry, automobile industry, ship industry et al. It formed a series of standards and norms, such as MIL-STD-1629A.

FTA was first proposed by Bell Labs in 1961, and used for safety analysis in aerospace industry, petrochemical, machinery manufacturing, and other areas[9]. This paper didn't give detailed introduction about FMEA and FTA because both of them were widely used and had mature technical specifications.

The FMEA/FTA was simply introduced by following steps:

(1) System functional analysis. Making clear the content and scope of safety analysis. Determining the level of FMEA and the basic function item. Establishing the system's functional schematic diagram.

(2) FMEA. Carrying out FMEA on each basic function item. If the component's information was stored in database, its FMEA can be got from the database directly. Determining the next level impact, the severity of ultimate impact, and filling out the system's FMEA worksheets.

(3) Finding the critical components and the corresponding ultimate impact. The critical components were weakness of system and should get more attention.

(4) FTA. Selecting the ultimate impact event as top event, and carry out its FTA.

(5) Make conclusions by FMEA/FTA.

The FMEA/FTA method listed system failure modes to form the FT. It can effectively overcome the respective shortcomings of FMEA and FTA and solve the problems in safety analysis of nuclear power system.

3. BN based on FMEA/FTA

3.1. BN

BN was proposed by Pearl in 1986[10], which was first used in the field of artificial intelligence, and then had been rapid development in information technology, industrial, medical, economy, reliability, safety fields. One with N nodes BN consists of two parts:

(1) Mode structure, namely the N-node directed acyclic graph G. The nodes set $V=\{V_1\ldots,V_N\}$ represents variables that can be abstraction of any things, such as the equipment state, observations value, personnel operations, and so on. Directed edges between nodes represent the association relationship between variables, usually called causal relationship. For the directed edges (V_i,V_j), V_j is called the parent node of V_i, and V_i is called the child mode of V_j. The node without parent node is called root node, and node without child node is called leaf node. Parent node set is usually represented as $Pa(V_i)$.

(2) The relevant parameters, representing probability of root node and conditional probability between nodes. By the conditional independence assumption of BN, conditional probability distribution can be described as $P(V_i \mid Pa(V_i))$, which expresses the quantitative association between node and its parent nodes. The joint probability distribution of all nodes can be calculated when the priori probability of root nodes and conditional probability distribution is obtained.

Using the conditional independence of BN, we can greatly simplify the calculation. The joint probability distribution of variables can be expressed as:

$$p(V_1 \cdots V_N) = \prod_{i=1}^{N} p(V_i \mid Pa(V_i)) \tag{1}$$

3.2. The model of BN based on FMEA/FTA

The mode can be constructed by following steps:

(1) FT to BN. Constructing BN by FT from FMEA/FTA. The method proposed by Bobbio in the literature[5].

(2) Model checking and improvement. The model needed to check whether it has same nodes and the logical and causal relationship between nodes. The node can be deleted when it is individual independent and do not impact on system safety.

(3) Obtaining probability. Node's probabilities include root probability and conditional probability. This paper used Bayes estimate and Monte Carlo simulation to assess the probability of root nodes. The conditional probability can be determined by the probability importance of failure modes or determined by the method mapped fault tree into BN. The conditional probability can also be based on expert experience in the early period of the model.

(4) Model amendment. As the employ time increase and the accumulation of failure events of complex systems, the structure and parameters of the model needed to be amendment to make the model improved.

3.3. Bidirectional inference and sensitivity analysis

(1) Diagnostic inference

The marginal probability of V_i is:

$$p(V_i) = \sum_{\text{except}V_i} p(V) \tag{2}$$

According to Bayes theorem, when an event has occurred or evidence is found, the posteriori probability of other nodes can be calculated as follows:

$$P(V|e)=\frac{P(V,e)}{P(e)}=\frac{P(V,e)}{\sum_{V}P(V,e)} \tag{3}$$

And e was represented as a evidence.

When the top event had happened, the probability of causal events can be calculated by BN model. Diagnostic inference can be used to judge main cause of the top event. When e was the top event, equation(3) was diagnostic inference.

(2) Predictive inference

Predictive inference was used to judge the influence in top event of causal events. When the causal events happened, the probability of the top event can be calculated by BN model through equation(3).

(3) Sensitivity analysis

According to BN' bidirectional inference, the rate of change of top event caused by causal event can be calculated. It was called sensitivity analysis, and used to judge the weakness of nuclear power system.

4. Bayes assessment and Monte Carlo simulation

Estimating root nodes probability in BN model was an important content in BN learning. There were two major problems in root probability estimation. (1) Multi-distribution. Not all components' probability distribution function was exponential distribution. Some components' probability distribution function was other distribution, such as normal distribution. (2) Lacking data. Nuclear power safety analysis was a small sample problem. This paper used Bayesian estimation and Monte Carlo simulation to assess the root nodes probability. It was useful to solve the two major problems.

4.1. Exponential distribution

When root nodes' probability distribution function was exponential distribution, it was supposed that the sample data was $x_i(i=1,2,...,N)$, x_i's probability distribution function was:

$$f(x_i)=\lambda e^{-\lambda x_i},\ \lambda \text{ was represented as failure rate} \tag{4}$$

According to the relationship of exponential distribution and Γ distribution[12], it can be gained:

$$x_i \sim \Gamma(1,\lambda) \tag{5}$$

So its summation was:

$$\sum_{i=1}^{N} x_i = \Gamma(N,\lambda) \tag{6}$$

Choosing λ's conjugate distribution as:

$$\pi_0(\lambda)=\Gamma(\lambda|\alpha_0,\beta_0) \tag{7}$$

And α_0,β_0 was super parameter.

According to Bayes equation, we can get:

$$\pi\left(\lambda\Big|\sum_{i=1}^{n}x_i\right)=\Gamma\left(\lambda\Big|n+\alpha_0,\beta_0+\sum_{i=1}^{n}x_i\right) \tag{8}$$

Given the confidence degree as $1-\gamma$, the Bayes upper limit of λ should meet the next equation.

$$1-\gamma=\int_0^{\lambda_u}\Gamma\left(\lambda\Big|n+\alpha_0,\beta_0+\sum_{i=1}^{n}x_i\right)d\lambda \tag{9}$$

So the probability of root nodes at time x was as follow:

$$F(x)=1-\exp(-\lambda_u x) \tag{10}$$

4.2. Normal distribution

When root nodes' probability distribution function was normal distribution, it was supposed that the sample data was $y_i (i = 1, 2, ..., N)$, and σ was known.

So

$$y_i \sim N(\mu, \sigma^2) \tag{11}$$

And μ 's conjugate distribution was:

$$\pi_0(\mu) = N(\mu_0, \sigma_0^2), \quad \mu_0, \sigma_0 \text{ was super parameter} \tag{12}$$

So

$$\overline{Y} = \frac{1}{n}\sum_{i=1}^{n} y_i = N(\mu, \sigma^2 / n) \tag{13}$$

Its likelihood function was the below equation.

$$L(\overline{Y} \mid \mu) = \frac{\sqrt{n}}{\sqrt{2\pi}\sigma} \exp\left\{ -\frac{n(\overline{Y} - \mu)^2}{2\sigma^2} \right\} \tag{14}$$

According to Bayes equation, we can get:

$$\mu \sim N(\mu_1, \sigma_1) \tag{15}$$

And

$$\mu_1 = \frac{\sigma^2 \mu_0 + n\sigma_0^2 \overline{Y}}{\sigma^2 + n\sigma_0^2}, \quad \sigma_1^2 = \frac{\sigma^2 \sigma_0^2}{\sigma^2 + n\sigma_0^2} \tag{16}$$

So the probability of root nodes at time y was as follow:

$$F(y) = 1 - \Phi\left(\frac{y - \mu}{\sigma} \right) \tag{17}$$

4.3. Monte Carlo simulation

Data lacking was a problem in root nodes estimation in nuclear power BN model. This paper used Monte Carlo simulation based Bayesian estimation. Monte Carlo simulation was suit for the small sample problem. We took exponential distribution as example to show the step of simulation. The cumulative distribution function of λ was:

$$F(\lambda) = \int_0^{\lambda} \Gamma\left(\lambda \middle| n + \alpha, \beta + \sum_{i=1}^{n} x_i \right) d\lambda \tag{18}$$

We used r_i to represent the random variable that arbitrary given in uniform distribution of the interval (0,1). According to $F(\lambda_i) = r_i$, one sample values can be got. So the step of Monte Carlo simulation based on Bayesian estimation was as follow.

(1) The simulation times began when $i = 1$. The random number r_i was sampled in the interval (0,1).

(2) Solved the equation $F(\lambda_i) = r_i$, the sample values λ_i was get.

(3) Repeating the step (1) and (2), the simulation can be stopped at the appointed simulation times N.

(4) Sorting the sample values as $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_N$. When the confidence degree was $1 - \gamma$, the λ_U (upper limit of failure rate) was the integral part of $(1 - \gamma)N$. So the root nodes probability can be calculated by equation (10).

5. A case study

The main function of reactor protection system was protect three major security barriers which were fuel cladding, a loop pressure boundary, containment. When the operating parameters exceed the threshold value of three major security barriers, the reactor protection system triggered *reactor scram* and started the security equipments.

According to the Fault Tree based on FMEA/FTA, the BN model of reactor protection system in Daya Bay nuclear power plant was constructed.

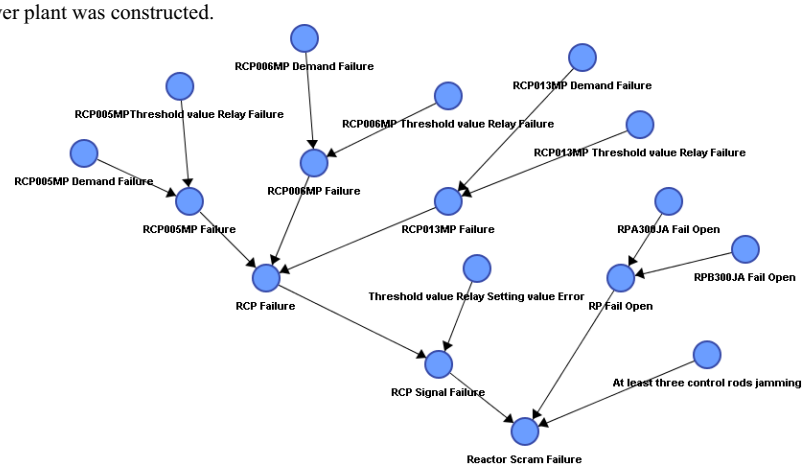

Figure1 The BN model of reactor protection system in Daya Bay nuclear power plant

The root probability was listed in table1[13].

Table 1 Probability of root nodes

Root nodes	Probability	Root nodes	Probability
RCP005MP Demand Failure	6.13E-03	RCP013MP Threshold value Relay Failure	1.00E-04
RCP005MPThreshold value Relay Failure	1.00E-04	Threshold value Relay Setting value Error	1.50E-04
RCP006MP Demand Failure	6.13E-03	RPA300JA Fail Open	3.20E-04
RCP006MP Threshold value Relay Failure	1.00E-04	RPB300JA Fail Open	3.20E-04
RCP013MP Demand Failure	6.13E-03	At least three control rods jamming	1.00E-04

The probability of *Reactor Scram Failure* was 1.521×10^{-3}, and the result was the same as calculated in literature[13]. According to BN sensitivity analysis, it was shown that *RCP Failure* was the major reason to cause the top event happen, and human error of *Threshold value Relay Setting value Error* was another major reason. So the two reasons should be attached importance to safety management.

BN method expanded the traditional safety methods in following way.

(1) Expand two states to multi state. FTA only deals with two state system, normal and fault. But most complex systems and their component had multi state practical when the systems or components were polymorphic, it simply need modify the corresponding node property in BN model.

(2) Dependence failure. One assumption of the fault tree was events were independent. For most of the complex systems, this assumption was not established. FMEA and FTA was hard deal with dependence failure. When the failure correlation, it also just need modify the node's conditional probability[11].

(3) Uncertainty. FMEA and FTA can't deal with uncertainty, but BN only need to modify the conditional probability of the corresponding node.

(4) Bidirectional inference. FMEA and FTA were one-way analysis method. FMEA/FTA is really not a bidirectional analysis. The BN' basic theoretical derived from the Bayesian formula, and can easily make causal inference and diagnostic inference. BN' bidirectional inference not only can quickly get the probability of the

occurrence of every node, but also can be used to find system's weaknesses, to provide a reliable evidence for the complex system safety analysis.

6. Conclusion

According to the problems of safety analysis in nuclear power systems, this paper proposed the BN method for nuclear power system. The BN model was constructed by the integration of FMEA and FTA (FMEA/FTA). This method can conveniently use bidirectional inference and sensitivity analysis to find the weakness of nuclear power system. To address the BN model multi-distribution and lacking data problem, this paper applied Bayes estimation and Monte Carlo simulation to assess probabilities of root nodes. The case study had shown the accuracy of the method. The BN method not only solved the shortcoming of traditional methods, but also had more advantages in safety analysis of complex nuclear power system. Using BN to model the dynamic system is the next important content in our research.

References

[1] Liu Xing-tang, Liang Bing-cheng, Liu Li, et al. The Theory, Method & Technique for Complex System Modeling. Beijing: *Science Press.* 2008; in press.
[2] Bluvband Z, Polak R, Grabov P. Bouncing Failure Analysis. *The Unified FTA-FMEA Methodology*, *IEEE RAMS* 2005; in press.
[3] Robyn R Lutz, Robert M Woodhouse. Requirements Analysis Using Forward and Backward Search. *Annals of Software Engineering* 1997; 1-18.
[4] Robyn R Lutz, Robert M Woodhouse. Bi-directional Analysis for Certification of Safety-Critical Software. ISACC'99, *International Software Assurance Certification Conference, Chantilly, VA,* 1999; 1-9.
[5] Bobbio A, Portianl L, Minichino M, et al.. Improving the analysis of dependable systems ty mapping fault trees into Bayesian Networks,"*Reliability Engineering and System Safety.* 2001; **71**: 249–260.
[6] Burton H Lee. Using Bayes Belief Networks In Industrial FMEA Modeling And Analysis. *Proceedings Annual Reliability and Maintainability Symposium, IEEE Press.* 2001; 7-15.
[7] Burton H Lee. Failure Modes and Effects Analysis with Bayesian Belief Networks.Bridging the Design-Diagnosis Modeling,USA; *Stanford University* 2002.
[8] Steven Kmenta, Kosuke Ishii.Scenario-based FMEA: a Life Cycle Cost Perspective. *ASME Design Engineering Technical Conference, USA: Maryland.*2000; 1-11.
[9] Michael Stamatelatos, William Vesely, Joanne Dugan, et al.. Fault Tree Handbook with Aerospace Applications USA: *Washington, DC*, 2002.
[10] Zhang Lian-wen, Guo Hai-peng. Introduction to Bayesian Networks Beijing. *Science Press.*2006; in press.
[11] Helge Langseth, Luigi Portinale.Bayesian networks in reliability.*Reliability Engineering and System Safety*. 2007;92:92-108.
[12] ZhouYuan-quan, Weng Chao-xi. Reliability Assessment Beijing: *Science Press* 1991; in press.
[13] YU Wen-ge, ZHANG Zhi-jian, HUANG Wei-gang et al.. Reactor Protection System Reliability Analysis of Daya Bay NPP, *Nuclear Power Engineering*. 2003; **24**: 63-67.