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.
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.