Annals of Nuclear Energy 110 (2017) 805–817

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Module level reliability performance evaluation of digital reactor protection system considering the repair and common cause failure

Zhanguo Ma [a,*], Hidekazu Yoshikawa [a], Ming Yang [a,b,*]

[a] Fundamental Science on Nuclear Safety and Simulation Technology Laboratory, College of Nuclear Science and Technology, Harbin Engineering University, 150001 Harbin, Heilongjiang, China
[b] School of Electric Power, South China University of Technology, 510641 Guangzhou, Guangdong, China

ARTICLE INFO

Article history:
Received 28 April 2016
Received in revised form 27 May 2017
Accepted 24 July 2017

Keywords:
Digital reactor protection system
Fault tolerance design and fault coverage
Reliability performance
Common cause failure

ABSTRACT

The Reactor Protection System (RPS) is designed and installed in the nuclear power plants (NPPs) to ensure both safety and economy. Nowadays the RPS adopts the digital techniques which consist of different digital modules. Therefore, this paper focuses on evaluating the reliability performance of the digital RPS using the Colored Petri Net (CPN) considering the module repair time whenever it fails and the Common Cause Failure (CCF). The module repair is considered as it takes some time to repair or replace the failed module and during the repair duration the digital RPS is operated in the degraded configuration and the common cause failure would severely impact the system in the event of occurrence. By studying the failure phenomenon and mechanism, the random probability shock model is adopted for CCF. Using the proposed model, the Monte Carlo simulation is carried out. Consequently, the indicators such as Mean Time To Repair (MTTR), Mean Time Between Failures (MTBF), Probability of Failure on Demand (PFD) and Probability of Spurious Trip (PST) are calculated. Following main conclusions are drawn i.e., i) the CCF is the main contribution to the PFD and PST. So the countermeasure for the CCF must be designed for the digital RPS; ii) the CCF has no effect on the MTTFF, MTBF, MTTR and subsystem unavailability; iii) the failure detection time has adverse effect on the system. Therefore, the digital system should shorten the detection time or decrease the coverage for the failures that take long time to be detected.

1. Introduction

The digital Reactor Protection System (RPS) automatically trips the reactor to maintain the reactor core integrity and the reactor coolant system pressure boundary when the plant process variables approach the specified safety limited conditions (Mitsubishi Heavy Industries Ltd., 2011). The digital RPS is designed following the regulations and standards (IEEE, 2009). The current dominant digital RPS is configured four identical trains. Each train consists of modules such as input modules, which acquire the process variable value from the sensor; logic calculation modules, which calculate the bistable and coincidence logic; communication modules that interchange the data between the trains or with other systems; and output modules, which actuate the actuator.

There are some basic requirements for the digital RPS design such as single failure criterion, redundancy, defense-in-depth and diversity, independence and so on (IAEA, 2011). Following the requirements, the fault tolerance technique (Dugan and Trived, 1989) is one of the important digital designs as it improves the performance and reliability of the system in nuclear power plants (NPPs). The fault tolerance techniques and their fault coverage are considered while evaluating the reliability of the digital RPS.

As the digital RPS is the important system, a lot of effort is focusing on the reliability assessment of the system in NPPs. The traditional methods (Gustafsson, 2012; Lee et al., 2006; Chu et al., 2008, 2009) such as event tree/fault tree method, Markov method, and failure mode and effect analysis are on trial. But it is demonstrated that traditional methods are useful but also have some limitations such as the time of event in accident sequences and interactions with the plant process cannot be modeled. At the same time, the dynamic methods (Aldemir et al., 2006, 2007, 2009, 2010) are surveyed and tried to evaluate the reliability of the digital RPS and it is suggested that the dynamic flowgraph methodology and Markov/cell to cell mapping are the recommended methodologies to model the digital instrumentation and

* Corresponding authors at: School of Electric Power, South China University of Technology, 510641 Guangzhou, Guangdong, China (M. Yang). Fundamental Science on Nuclear Safety and Simulation Technology Laboratory, College of Nuclear Science and Technology, Harbin Engineering University, 150001 Harbin, Heilongjiang, China (Z. Ma).

E-mail addresses: mazhanguo2013@163.com (Z. Ma), yangming@hrbeu.edu.cn (M. Yang).

http://dx.doi.org/10.1016/j.anucene.2017.07.025
0306-4549/© 2017 Elsevier Ltd. All rights reserved.

control system. The research tries to find the methodology to model the digital system. But now there is no consistent agreement on the methodology.

In this paper, an attempt is made to model the digital RPS using the formal modeling methodology – Colored Petri Net (CPN) from the module level. The Petri Net and Colored Petri Net informal definition and relations are explained in Zhanguo et al. (2015a,b) and Jensen (2007). In the model, the fault tolerance design techniques are considered and the detection time of the failure and repair time of the failed modules are modeled and the effect on the system is analyzed.

In the authors' research, it is found that the independent failures can cause one train and two trains failure. And the Common Cause Failure (CCF) is the main contribution to the three trains and four trains failure. And the study in Kang and Sung (2002) also pointed that the cutsets which contain CCF events are the main contributor to the RPS unavailability. When modeling the CCF for the digital RPS, the β model is commonly adopted (Lilleheier, 2008; Jin et al., 2016). But it is conservative. The digital RPS is usually designed to configure 4 identical subsystems and each subsystem is configured several modules. So there are dozens of or hundreds of modules in the digital RPS. When the CCF event occurs, some of the modules are impacted and cannot perform their functions while other modules are not affected at all. This kind of CCF event has partial effect on the system and it is defined as the nonlethal CCF. While some CCF events may have impact on all the modules, so that the system is surely failed and this kind of CCF is defined as lethal CCF. Furthermore, even though different CCF events are classified as nonlethal CCF events, they may have different severe level of effect on the system that is to say the modules have different failure probability during different nonlethal CCF events. Considering the failure phenomenon and mechanism, the random probability shock model (Atwood, 1986; Atwood and Kelly, 2009) is very well adapted to represent the CCF effect.

The objective of this paper is to develop the CPN models for the digital RPS considering both the repair time and CCF effect in the module level. Then the Monte Carlo simulation is performed and the reliability performance such as the system unavailability, mean time to first failure (MTTFF), Mean Time Between Failure (MTBF), Mean Time To Repair (MTTR) for each train and the Probability of Failure on Demand (PFD) and Probability Of Spurious Trip (PST) for RPS, which represent the system safety and economy respectively, are calculated. The rest of the paper is organized as follows. The fault tolerance design techniques and fault coverage is briefly introduced in Section 2. In Section 3, the common cause failure model is introduced from binominal failure model to the random probability shock model. The detailed CPN models for the example digital RPS are presented in the Section 4. Section 5 presents the simulation results of the example digital RPS reliability performance. In Section 6, the conclusions are given.

2. Fault tolerance techniques and fault coverage

In order to calculate the failure rates for different kinds of failure, the fault tolerance techniques are introduced to identify different failures and calculate the corresponding failure rates. The fault tolerance techniques not only enhance the safety and reliability but also alleviate the maintenance for the digital system. The fault tolerance is the system's property that enables a system to correctly perform the specific required function in the event of failure of the components or sub-system. The fault coverage is the evaluation of the fault tolerance design and it is the ability to perform fault detection, fault isolation and fault recovery. The mathematical definition of the fault coverage is the conditional probability of a fault detection and recovery given that the fault exists in the system as shown in Aldemir et al. (2007).

$$C = \Pr\ (\textit{fault detected}|\textit{fault existence}) \tag{1}$$

In fact, there are several kinds of fault tolerance design in the digital system for different faults. The specific fault tolerance technique can detect and recover certain faults. So it is important to clearly know the fault coverage for each fault tolerance technique. The fault coverage is usually obtained by the fault injection experiment (Hsueh et al., 1997).

Certain faults may be detected by several fault tolerance techniques, and some certain faults may not be detected by any fault tolerance techniques. As the different fault techniques are running at the same time, different fault tolerance designs may act as the different levels of barrier in case of some fault tolerance technique failure. In the paper, if a fault is detected by several fault tolerance techniques, the coverage for the fault is classified to the fault tolerance technique which detects the fault first. Then the coverage for each fault tolerance technique is explicit.

For each fault tolerance technique *i* in the system, the fault coverage is C_i. The failure rate corresponding to the fault tolerance technique is calculated using the failure rate of the system and the fault coverage.

$$\lambda_i = C_i \cdot \lambda_s \tag{2}$$

where λ_i is the failure rate that is covered by the *i*th fault tolerance technique, λ_s is the failure rate of the system.

It is assumed that 100% of the failures are detected by the different fault tolerance techniques. And for all failures, the failed modules can be repaired or replaced. After repair the digital system is working as good as new.

3. Common cause failure model

The random probability shock model is very well adapted to represent the CCF effect on the digital RPS and the random probability shock model is introduced based on the Binomial Failure Rate (BFR) model. So the BFR model is first introduced and then random probability shock model is introduced.

3.1. Binomial failure rate model

In the BFR model, two kinds of common cause shocks are defined: nonlethal shocks and lethal shocks (Atwood, 1986; Atwood and Kelly, 2009). When a nonlethal common cause shock occurs, some of the components are failed. Each component is failed independently of other components with the probability ρ. The number of failed components k_{ccf} is random and follows the binomial distribution.

$$f_{k_{ccf}} = \binom{N_c}{k_{ccf}} \rho^{k_{ccf}} (1-\rho)^{N_c - k_{ccf}} \tag{3}$$

where, $f_{k_{ccf}}$ is the probability of k_{ccf} components fail when a nonlethal shock occurs, N_c is the total number of the components in the system.

A lethal shock is an event that impacts every component in the system to fail, not a random number of components. The nonlethal and lethal shocks are assumed to occur independently of each other. The time between the nonlethal shocks is assumed to be exponentially distributed with the nonlethal shock rate v. And the time between the lethal shocks is also assumed to be exponential distributed with the lethal shock rate ω.

For a specific component in the system, the failure rate is given by:

$$\lambda_1 = \lambda_{ind} + v\rho + \omega \tag{4}$$

where λ_1 is a specific component failure rate, λ_{ind} is the independent failure rate of the component.