International Journal of Engineering & Technology, 7 (2.12) (2018) 210-213

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Probabilistic safety assessment (PSA) of a safety critical system: a case study of a nuclear power plant

Vinay Kumar [1] *, Dewanshu Pratihar [1], Anil Kumar Tripathi [1]

[1] Indian Institute of Technology (BHU), Varanasi, India
**Corresponding author E-mail: vinay.rs.cse13@iitbhu.ac.in*

Abstract

Probabilistic Safety Assessment approach has been successfully applied in engineering, economics, computer science and statistics to resolve a wide range of safety-related problems. However, using Probabilistic Safety Assessment for quantifying safety of a safety critical system is a challenging task in Safety Engineering community. This method plays an essential role in analyzing safety of safety critical sys-tems and its various components. Therefore, in this paper, we present Probabilistic Safety Assessment framework which can be used to quantify the critical failures of a systems. The approach is well demonstrated on a Digital Feed Water Control System uses in a Nuclear Power Plant as safety critical system.

Keywords: *Common Cause Failure (CCF); Nuclear Power Plant (NPP); Probabilistic Safety Assessment (PSA); Safety Critical System.*

1. Introduction

Nowadays, Safety critical system plays an important role as instrumentation and control system whose failure may cause intensive environment damage, significant financial loss, and threat to human lives. There are numerous examples of accidents of large scale [1], [2] like those at the Chernobyl nuclear plants, Three Mile Island and, the Bhopal pesticide plant gas leak and the explosion of Challenger space shuttle. These failures occur due to many types of causes which include faulty manufacturing, bad engineering design, inadequate testing, poor maintenance, improper use, and human error. Therefore, dependability attributes, viz. safety, reliability, and security of such system should be high for user's confidence in that system to use. Safety critical systems are installed everywhere nowadays such as medical equipment, military equipment, navigation systems, power plants, and many more. Losses are very high for such system failures. Therefore, safety aspects are one of the prime concern in the design and architectural phases of system development life cycle. Safety engineering is a discipline in the field of engineering, which helps in ensuring that acceptable levels of safety are being provided in the engineered systems.
Safety [3], [4] can be described as capability of a component, not to result in or lead to endangerment of people in a specific condition or a period of time. A safe system holds both of these conditions simultaneously:

- There is not a possibility of a hazardous operation or has no endangering consequence.
- The component can be used without any endangering events or consequences.

The remainder of this paper is as follows: In section 2, we give the background details and related work for safety analysis of the systems. A proposed approach along with its framework model for quantification of safety is given in the section 3. Section 4 describes our experimental Setup and results for DFWCS as a case study of NPP. Section 5 concludes this paper.

2. Background details and related work

In the past, Nuclear power plants (NPPs) were based on analog machines for surveillance, safety and control operations. Due to Technological advancement from analog to digital systems, for their operational benefits, plants have started initiating changes like these too. Meanwhile newer NPP designs are already incorporating the usage of digital systems. Now that digital instrumentation and control mechanisms are an essential part of safety of a nuclear power plant, the US Nuclear Regulatory Commission (NRC) has come up with a research plan for digital system which provides a list of research plans for providing support to its regulatory requirements.
The major aim of the NRC plan on risk assessment techniques and information regarding digital systems is to find out techniques, analytical toolkit, and regulatory supervision to sustain: (1) Inclusion of models concerning digital systems, for PRA and (2) Usage of information accessible about the risks incorporated in digital systems of NPP. In particular, the reliability of digital IC systems is being analysed by the NRC, using traditional and dynamic (non-traditional) techniques simultaneously. This kind of traditional methodology is demonstrated by the Event Tree or Fault Tree methodology.
In the recent past, Brookhaven National Laboratory (BNL) has made some progress in development of analysis techniques and procedures for digital systems and modelling their probabilities for NRC projects. This development incorporates re-examining the literature based on digital system modelling [5 - 7], detailing and investigating knowledge of working of digital systems [6], carrying out quantification of malfunction rates incorporating a Hierarchical Bayesian Method [8], and using Failure Modes and Effects Analysis. These analysis provide information that breakdown of these systems have resulted in many hazards which eventually contributed in either a machinery damage or a reactor failure at NPPs, and at least a single hazard at a Nuclear Power Plant due to which a

small coolant accident occurred while re-fuelling [NEA 1988], and a lot of events which caused accidents in several plants and factories. NUREG [7] documents the preparation of the list of features to be considered for assessing reliability models for digital systems, i.e. how to choose the traditional reliability methodologies, and development of the process for performing the reliability analysis of a DFWCS. For trial application, two reliability models, the traditional Markov method and the Event/Fault Tree method were selected. The usage of latter is common in NPP industry all across the world. Vinay et al. [9-12] proposed a framework for the assessment of dependability attribute like reliability and safety of as safety critical (and control) system's software. All the approaches is well illustrated with an NPP system as case study along with experimental validation. Therefore, such approach can be used for complex safety critical system.

3. Proposed approach

PSA, is being used and applied extensively in various fields. This approach is being used all over the world in nuclear facilities, aerospace, the chemical and process plants, and nowadays, even in the field of financial management. The aim of PSA to identify the events and the combination(s) of these events which can lead to accidents of large-scale, assessing each combination and its probability of occurrence and evaluation of the consequences. PSA also includes the quantitative estimation of risk which is useful for comparing alternatives in different engineering and design areas.
In spite of the benefits, PSA has its own well-known restrictions. Characteristics which are uncertain in nature, like informative models on common-cause failures (CCFs) affect the precision of the PSA. Therefore, we proposed a framework for the quantification of various failures of a safety critical system. This framework is based on hybrid modelling technique that uses features of Fault tree method as well as Event tree method. The framework is shown in Fig. 1.

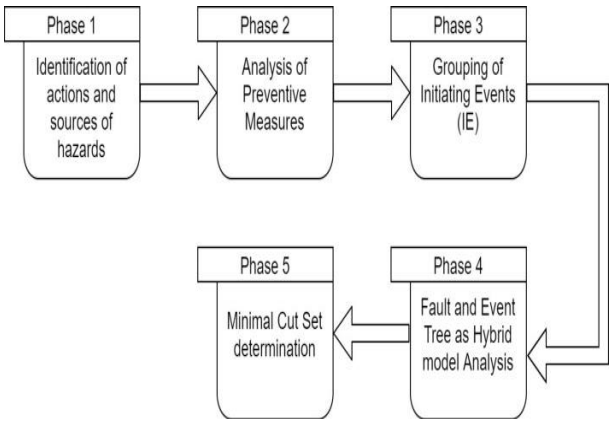

Fig. 1: A PSA Framework.

4. Experimental setup and results

A Case Study: DFWCS
PWR: Pressurized Water Reactor
DFWCS: Digital Feed-water Control
CPU: Central Processing Unit
FWP: Feed-water Pump
MFV: Main Feed-water valve
BFV: Bypass Feed-water valve
PDI: Pressure Differential Indicating

4.1. DFWCs overview

Digital Feed-water Control System's primary function is to regulate the flow of feed-water during normal at-power operations, and optionally during plant heat up or cool down. The schematic diagram shown in Fig. 2. Both secondary loops of a PWR consists of digital DFWCS. One of these similar DFWCSs is analyzed.
The DFWCS comprises of the two CPU modules (i.e. the backup and main CPUs), transmitters, sensors, and modules for controlling system. The FWP, MFV, BFV, and PDI are all allocated one controlled module each. DFWCS also consists of support systems, i.e., 120v alternating current (AC) buses and direct current (DC) power supplies. The main and bypass feed water-regulating valve (i.e. MFRV and BFRV) and their positioners, and the main feedwater pump (MFP)'s turbine controller receive demand signals from the DFWCS. The valves are positioned by the positioners through conversion of electrical signals into pneumatic pressure. The main function of PDI is to log and report by displaying the variation in pressure across the MFRV. The System's digital parts, which are modules for CPU and controlling, each comprises of a microprocessor and the components associated to it, For example, multiplexer, analog to digital and digital to analog converter.

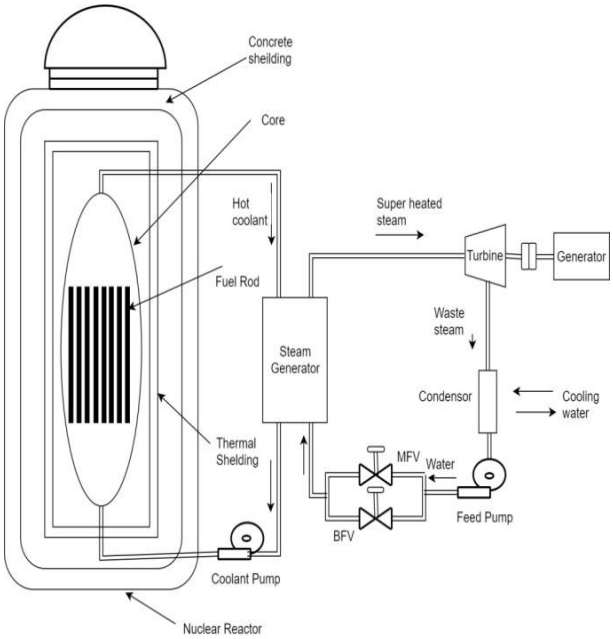

Fig. 2: The DFWCS System Outlay.

4.2. DFWCS operation

It is Assumed that initially, the mode of operation of system is automatic. The system can also be operated in manual mode. In case of an emergency or failure, the mode is switched by the controller from automatic to manual and the operators can then take manual control. The main control room also consists of controllers, through which the operators can achieve manual interaction with the system. It is assumed in this case study, that since automatic control is lost, a transfer to manual mode is failure of a system.

4.3. DFWCS operating modes

The DFWCS operates in two modes i.e. low-power or high-power mode. While operating on full power, The DFWCS usually performs its operations under the control of three element, in which based on Inputs from various kinds of sensors the control is determined, which includes, steam flow, feedwater flow, and steam generator level. These signals (three types) act as input signals to the sensor of DFWCS and play a very important role in its functioning. In this study, it is assumed that the plant is working at its maximum power. Hence, initially, the system is assumed to be working in the high-power mode.

4.4. Different phases of proposed framework

Phase 1: Identification of actions and sources of hazards

In In this step, all the sources of hazard like fire, hazardous substances, radioactivity, etc., which can contribute to accidents, are found out and a list is made. This process of identification of the hazards or accident initiation can be done using several approaches like master logic diagrams (MLDs), preliminary hazard analysis (PHA), failure mode and effect analysis (FMEA), and HAZOP.
Here, we use PHA for Identifying Actions and hazards. It is used in preliminary design stage and it helps in identification of system's major hazards or endangering events, its severity and its consequences and given in Table 1.

Table 1: PHA of A DFWCS

Hazardous element	Event causing hazardous situation	Hazardous situation	Event leading to potential accident
Software	Common causes	Software CCF (Common cause failure)	Fault in program
Hardware	Common causes	Hardware CCF (Common cause failure)	Improper care of hardware
Main CPU software	Aging of software	Erroneous outputs by software	No regular updates
Main CPU Software	Improper monitoring of operation	Software halts (CPU stops updating output)	Bugs in software
ISA bus	Fault in ISA bus	Loss of ISA bus	Damage to hardware
Power Supply	Variation in Power supply voltage	Failure of voltage signal	No power supply

Phase 2: Analysis of preventive measures
In this phase, Preventive measures for all the hazards or actions are identified after obtaining the information from the employees or officials working in the NPP. This information is then organized and tabulated as shown below in Table 2.

Table 2: Preventive Measures Identified

Potential accident	Effects	Preventive measures
System failure	System stops working	Proper development of software
System failure	System stops working	Proper safety measurements
Fails entire system	System failure	Provision of regular updates for the software
WDT no longer receives signal. Failover to Backup CPU.	Backup CPU starts operating	Regular checks for bugs in software.
Loss of input and output in CPU	Improper functioning of system	Using good quality microprocessor
Loss of automatic control	Shift to manual control and system failure	Uninterrupted Power Supply and Reliable Power Source

Phase 3: Grouping of initiating events (IE)
Initiating Events are identified from the Information collected about the system in Phase I and grouped into different categories and shown in Table 3.

Table 3: Grouping of Initiating Events

Group	Events
Common Cause Failure	Software, Hardware CCF
Loss of Automation	Voltage signal drift and A/D converter failure.
Software Halt	Software stops working
Microprocessor fault	Loss of ISA Bus
Power Supply loss	Unavailability of Power Supply

Phase 4: Fault and event tree as hybrid model analysis
In this phase responses are explored through a single initiating event and a path is laid down for probabilistic assessment of the results and analysis of the overall system. The effects of functioning or failed systems can be analyzed using this technique, given that an event has occurred. Fig. 3 shows the hybrid model based on Fault and Event tree for DFWCS. For the quantification of safety, we have required all the failure rates of individual components therefore, these real data is collected from NUREG/CR-6997 (BNL-NUREG-90315-2009) [13] which is shown in Table 4.

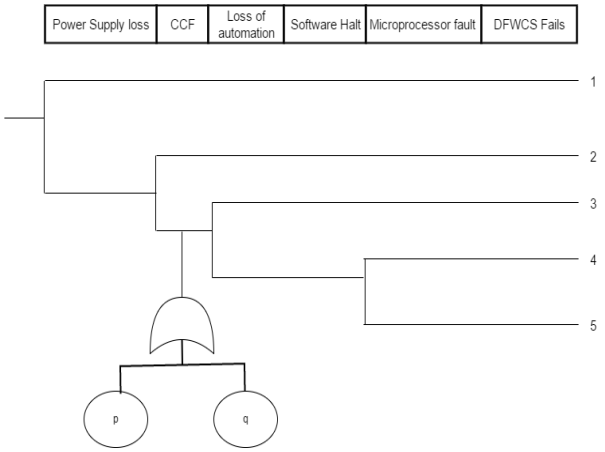

Fig. 3: Event Tree of DFWCS Failure [P: Probability of Software CCF; Q: Probability of Hardware CCF].

Simple elementary events or a complicated system can act as the pivotal events (Event tree's branches). These systems have a possibility of requirement of fault tree for calculation of minimal cut sets. Boolean algebra rules are used to determine the minimal cut set expression for each accident sequence.

Table 4: Probability of Occurrence of All the Failure Events Fordfwcs

EVENTS	PROBABILITY OF OCCURRENCE
Power Supply Loss	$1.0 * 10^{-5}$
Software CCF	$5.0 * 10^{-10}$
Hardware CCF	$7.3 * 10^{-7}$
Loss of Automation	$5.0 * 10^{-7}$
Software Halt	$1.3 * 10^{-9}$
Microprocessor Fault	$5.2 * 10^{-7}$

Phase 5: Minimal cut set determination
Cut sets are the unique combinations of component failures that can cause system failure. A minimal cut set is basically a cut set from which any basic event is removed, and the left out events together are not anymore a cut set.
Minimal cut sets provide deep understanding about a system's structural vulnerability. The length of a minimal cut set is inversely proportional to the vulnerability of the system (fault tree's top event) to that combination of events. Single point failures (one autonomous component of a system which causes the failure of entire system) can be discovered using Cut sets. Table 5 shows the quantification of all the failures for DFWCS.

Minimal Cut Sets for the event tree of DFWCS:
Boolean expressions for the top events

$$S1 = I = 1.0 * 10\text{-}5$$

$$S2 = p + q = 5.0 * 10\text{-}10 + 7.3 * 10\text{-}7$$

$$S3 = c = 5.0 * 10\text{-}7$$

$$S4 = d = 1.3 * 10\text{-}9$$

$$S5 = e = 5.2 * 10\text{-}7$$

Sequence's Boolean expression

$$Seq1 = I = 1.0 * 10\text{-}5$$

$$Seq2 = 1 - I = 9.9 * 10\text{-}1$$

$$Seq3 = (1 - I) * (1 - (p + q)) * c$$

$$= 9.9 * 10\text{-}1 * 7.305 * 10\text{-}7 * 5.0 * 10\text{-}7$$

$$Seq4 = (1 - I) * (1 - (p + q)) * (1 - c) * e$$

$$= 9.9 * 10\text{-}1 * 7.305 * 10\text{-}7 * 0.99995 * 5.2 * 10\text{-}7$$

$$Seq5 = (1 - I) * (1 - (p + q)) * (1 - c) * (1 - e)$$

$$= 9.9 * 10\text{-}1 * 7.305 * 10\text{-}7 * 0.99995 * 0.99995$$

Table 5: Quantification of All the Failures for DFWCS

SEQUENCE	PROBABILITY
1	$1.0 * 10^{-5}$
2	$9.9 * 10^{-1}$
3	$4.9 * 10^{-7}$
4	$5.1 * 10^{-7}$
5	$9.7 * 10^{-1}$

From this table, we can observe that the highest failure rate of DFWCS is $9.7 * 10^{-1}$ whereas the minimum failure rate is $4.9 * 10^{-7}$.

5. Conclusions

Safety prediction approaches have been intensively studied in past decades. This results, many research papers based on safety analysis have been published. But, most of them unable to propagate the full information to understand a model due to lack of sufficient methodological and contextual celerity. Therefore, we proposed a framework for quantification of safety of a safety critical system based on hybrid model. This frame utilizes features of both Fault tree as well as Event tree method. The approach has been uses operational profile of various safety critical systems of NPP and in this paper; it is demonstrated on DFWCS. The result of the proposed approach shows its effectiveness.

References

[1] Wong W. Eric, Debroy Vidroha, and Restrepo Andrew, "The role of software in recent catastrophic accidents," IEEE Reliability Society 2009 Annual Technology Report, (2009), pp. 1-8,

[2] Sunanda B. Esther, Seetharamaiah P., "Modeling of Safety Critical Systems Using Petri Nets," ACM SIGSOFT Software Engineering Notes 40, no. 1, (2015), pp. 1-7.

[3] Lawrence J. Dennis, Software reliability and safety in nuclear reactor protection systems. Division of Reactor Controls and Human Factors, Office of Nuclear Reactor Regulation, US Nuclear Regulatory Commission, (1993).

[4] Goseva-Popstojanova Katerina, and Trivedi Kishor S., "Failure correlation in software reliability models," IEEE Transactions on Reliability 49, no. 1, (2000), pp. 37-48.

[5] Chu T. L., Martinez-Guridi G., Lehner J., and Overland D. Issues Associated with Probabilistic Failure Modeling Of Digital Systems. No. Bnl--72381-2004-Cp. Brookhaven National Laboratory, (2004).

[6] Chu T. L., Martinez-Guridi G., Yue M., and Lehner J. A Review of Software-Induced Failure Experience. No. Bnl--Nureg-77124-2006-Cp. Brookhaven National Laboratory, (2006).

[7] Chu T. L., Martinez-Guridi G., Yue M., Lehner J., and Samanta P. "Traditional Probabilistic Risk Assessment Methods for Digital Systems (NUREG/CR-6962)." US NRC, (2008).

[8] Yue Meng, and Chu Tsong-Lun. "Estimation of Failure Rates of Digital Components Using a Hierarchical Bayesian Method (PSAM-0320)." In Proceedings of the Eighth International Conference on Probabilistic Safety Assessment & Management (PSAM). ASME Press, (2006).

[9] Kumar Vinay, Singh Lalit Kumar, Tripathi Anil Kumar, and Singh Pooja. "Safety Analysis of Safety Critical Systems Using State-Space Models." IEEE Software 34, no. 4, pp. 38-47, 2017.

[10] Kumar Vinay, Singh Lalit Kumar, and Tripathi Anil Kumar. "Transformation of deterministic models into state space models for safety analysis of safety critical systems: A case study of NPP." Annals of Nuclear Energy 105, (2017), pp. 133-143.

[11] Kumar Vinay, Singh Lalit, and Tripathi A. K. "A Probabilistic Hazard Assessment Framework for Safety Critical and Control Systems: A Case Study for a Nuclear Power Plant." Nuclear Technology 197, no. 1, (2017), pp. 20-28.

[12] Kumar Vinay, Singh Lalit, and Tripathi Anil. "Reliability Analysis of safety critical and control systems: A state-of-the-art review." IET Software (online), (2017), pp. 1-18.

[13] Chu T. L., Yue M., Martinez-Guridi G., Mernick K., Lehner J., and Kuritzky A. "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Methods." Washington DC: US Nuclear Regulatory Commission, (2009).