Chapter 5

A Probabilistic Hazard Assessment Framework for the Safety Critical and control System

Any risk in safety-critical or control applications may lead to catastrophic disaster; hence, safety is a primary concern for such applications. In this chapter, we are going to demonstrate how a hazard based modeling of safety can be easily applicable to various possible Safety Critical System (SCS) and hence, we propose and describe hazard oriented model of SCS in this chapter. The impact of risk varies from minor inconvenience and cost to personal injury, significant economic loss, and death. Therefore, a safety assessment process should be an inherent part of the system development process to make a system safe or to ensure that the effects of failures are minimized. This chapter deals with a new probabilistic approach to quantify the safety of SCSs and control systems based on probabilistic safety assessment to

address the shortcomings of the existing techniques discussed in Section 4.2.1. The methodology has been tested on 29 operational data sets to validate its effectiveness. This chapter demonstrates the methodology on the Digital Feed Water Controller System (DFWCS) of a nuclear power plant (NPP). The results indicate that the method can identify possible hazards and quantify such hazards of a SCS.

5.1 Introduction

A SCS executes the critical tasks, the failure of which may jeopardize human life, lead to considerable financial misfortune, or cause extensive environmental damage lead to catastrophic disaster. Therefore, safety turns into a primal appraisal in safety-related systems where human lives can be, by some means, place in danger, expecting to agree to safety necessities defined by industry norms, like ANSI/ISA S84, IEC 61513, IEC 61496 (EN 61496). Safety analysis of the system has played a significant role in improving and verifying the safety of critical systems. However, the need of safety analysis is not restricted to predicting whether safety goals, can be grasped. It can be utilized for other goals as well disscussed in Chapter 1.

The research work in this chapter concentrates on the improvement of the current methodology to find out the safety-related hazards assessment of a SCS. In addition, this can be applicable to all types of system, provided if it is conceivable to design or model it. We have considered a part of system of pressurized water reactor (PWR), known as DFWCS as a case study.

The remaining part of the chapter is organization as follows. Section 5.2 discusses the current methodologies used for evaluating the hazards of safety-related or SCSs. It also identifies the limitations of these methodologies. In section 5.3, we propose a probabilistic approach for estimating the safety-related hazard of a computer-based system (CBS) based on the IEC 61508 as Safety Integrity Level (SIL). We demonstrate our approach with the help of a case study. In Section 5.4, we validate our approach. Section 5.5 concludes this chapter. To be able to use this model in actual calculations, hazards need to be determined and assigned a probability, determining how often they are believed to occur in this thesis work.

5.2 Related Work

Karol Rástočný and Juraj Ilavský [112] proposed a method to quantify the safety level of a safety-critical control system. This method uses Continuous Time Markov Chain (CTMC) analysis to find out hazardous failure rate of a safety control system. The one of the limitations of this approach is that it only considers hardware failures.

Yangyang Yu et al. [120] developed a technique for safety sensitivity analysis of the SCSs. This method is built upon a sensitivity analysis approach for acyclic Markov reliability models and the Markov Chain Modular approach. But, this approach works only for the system which modules are connected in a series configuration.

Y. Yangyang and Barry W. Johnson [123] introduce two safety-related metrics to evaluate a safety-critical CBS. Markov models are used to deriving these metrics. The authors assume that the failure rates of the some components are zero and treat them as perfect components during the lifetime of the system.

J. Börcsök et al. [125] proposed a paper: "How Safe is my System?" In this paper, the authors quantified many parameters, which are associated with safety. But, the proposed safety parameters have not been experimentally validated.

F. Ahmad et al. [126] proposed a method for specification and verification of safety properties based on Arc-constant coloured Petri net (ac-CPN). It gives a qualitative assessment of safety which works in a fruitful manner on non-critical systems, where reliability and safety requirements are not very stringent.

S. P. Kumar et al. [130] proposed a methodology for building safer software based critical computing systems. The technique does not give any quantitative performance indicators.

H. Pan et al. [131] proposed a method to model the soft-ware safety, and perform computation methods to analyze software safety at the system level, module level and function unit level. Due to a use of Markov model, authors assume state transition probability as constant.

Abdullah et al. [134] proposed an approach for hazard analysis of the SCS. The methodology comprises of three stages. This paper focuses only on identification of hazards sequentially. However, concur-rent hazards are possible in case of SCS.

G. Zhou and Huibing Zhao [133] proposed a methodology using FTA and colored Petri net for safety requirements analysis and performance verification. By using FTA in preliminary hazard identification process, we are unable to do the reconfiguration of a system after the detection of a failure or system recovery of the system.

R. J. Rodrıguez et al. [135] proposed a method that verifies the safety constraints from the early phase of SDLC. In this paper, they use UML for system design and Object Constraint Language (OCL) for Specifying safety contract. The verification is done using PN. But, defining the safety contracts in mathematical form would be a very cumbersome process, especially in complex systems.

Peng Li et al. [141] proposed automated state-space model generation of large-scale distribution networks for model order reduction. Their algorithm constructs models of large systems. However, validating the models requires a strong mathematical background.

Lalit Kumar Singh et al. [142] proposed a Markov chain approach for reliability analysis that can be extended to safety analysis. They presented an NPP case study and an experimental validation, but they didn't describe or validate creation of a Markov chain.

All of the above methodologies have taken are either qualitative or quantitative approach to safety analysis, where the applicability is restricted to logically feasible

models. However, these quantitative safety analysis methods are difficult to generalize.

5.3 The Proposed Method for Quantification of Hazards with a Case Study Illustration

In this section, We propose a framework for quantification of all the possible Hazards with the help of a DFWCS as case study. The overview of the DFWCS is already discussed in Section 3.3. We can utilize Our framework to know: 1) to what extent of the system is safe and 2) what types of the risks are associated with the system. We use this framework for the various SCSs. The Quantitative framework contains six phases as shown in Figure 5.1. Each phase is described as follows.

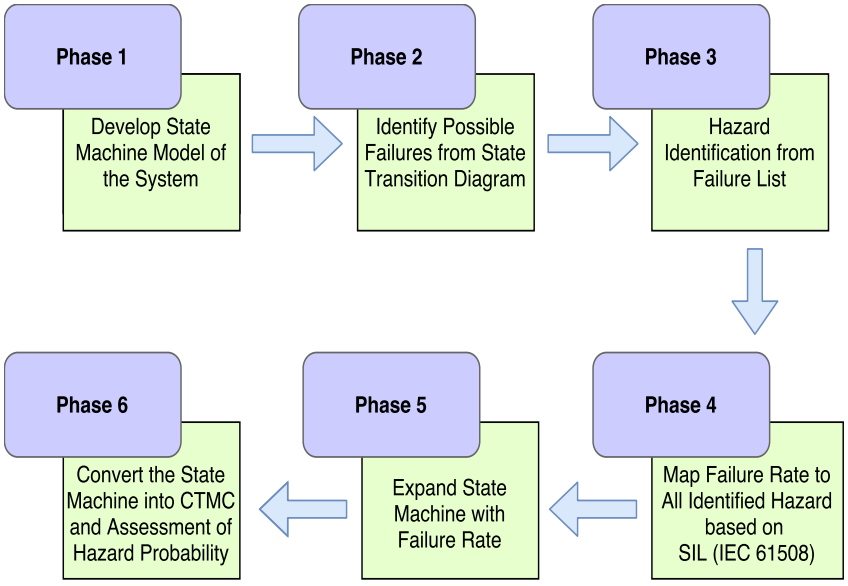

FIGURE 5.1: The Quantitative Hazard Assessment Framework

5.3.1 Phase 1: Develop State Machine Model of the System

In this phase, a state machine model of the system, of which hazard analysis is to be done, is developed based on the system specifications. State machines are capable of modeling all possible conditions of a system together with its related transitions. The state machines of DFWCS and the components are shown in Figure 5.2 and Figure 5.3.

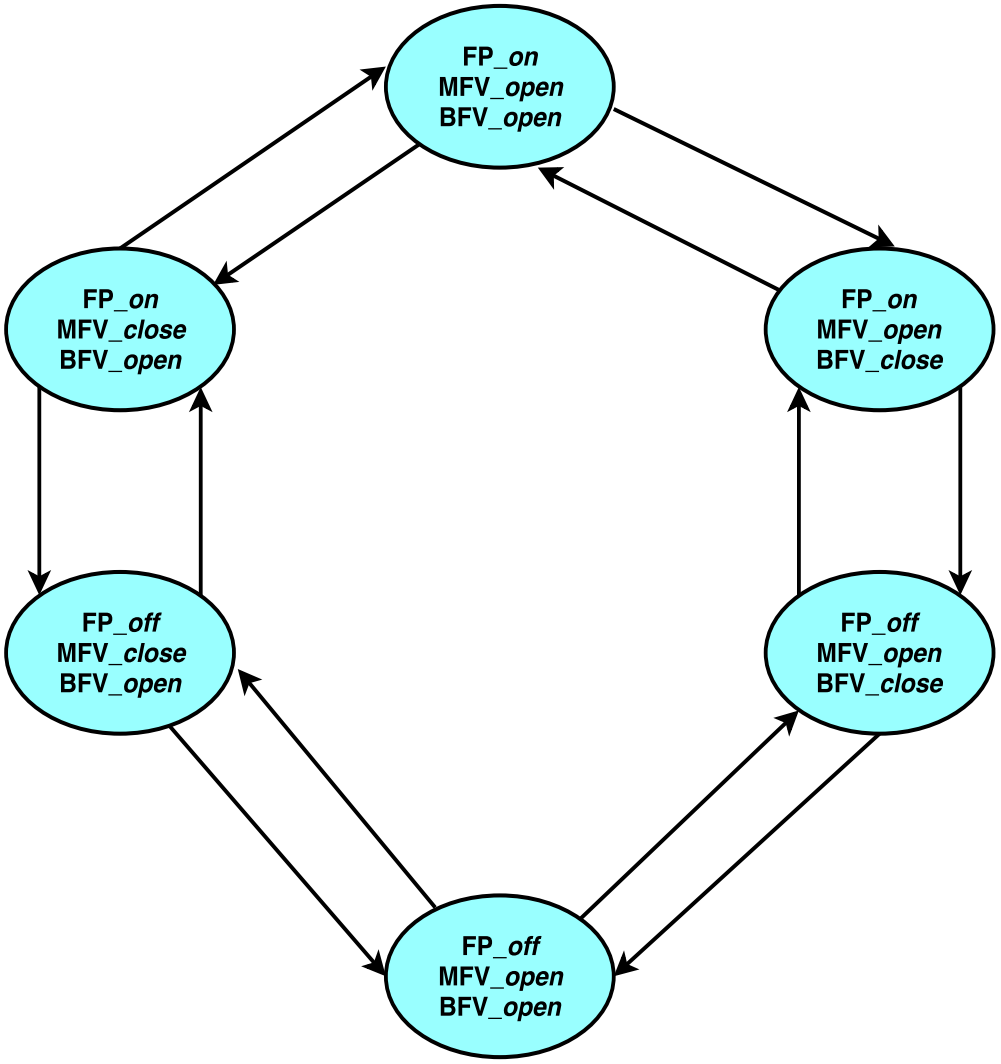

FIGURE 5.2: State Transition Machine of Digital Feedwater Control system

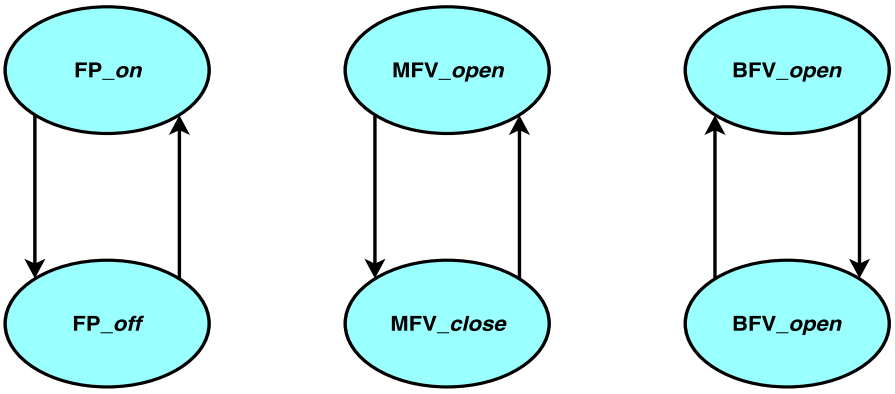

FIGURE 5.3: State Transition Machines of FP, MFV and BFV

5.3.2 Phase 2: Identify Possible Failures from State Transition Diagram

In this phase, we identify all possible failures to the system from the state machines transitions. These failures are identified using of qualitative approaches, such as check list, mind maps and etc. post analysis of these failures, some or all of them are identified as hazards ($failures \subseteq hazards$) depending upon no. of critical components used in state machines. Tables 5.1 show all the possible failures of DFWC system. Since, DFWC is a safety-critical system, therefore each failure lead to hazard, i.e. $failures = hazards$.

5.3.3 Phase 3: Identify Possible Failures from State Transition Diagram

In this phase, rigorous analysis required to find out all possible hazards not only form a single point of failure of system but also from multiple points of failures which

TABLE 5.1: Possible failures mapped to digital feedwater controller system

Component used in State Machines	Transition associated	Explanation	Hazard
MFV	MFV *close* $\rightarrow$ MFV *open*	MFV *open* when it should *close* & Previous state of MFV is *close*	H_1
	MFV *close* $\not\rightarrow$ MFV *open*	MFV *close* when it should *open* & Previous state of MFV is *close*	H_2
	MFV *open* $\rightarrow$ MFV*close*	MFV *close* when it should *open* & Previous state of MFV is *open*	H_3
	MFV *open* $\not\rightarrow$ MFV *close*	MFV *open* when it should *close* & Previous state of MFV is *open*	H_4
BFV	BFV *close* $\rightarrow$ BFV *open*	BFV *open* when it should *close* & Previous state of BFV is *close*	H_5
	BFV *close* $\not\rightarrow$ BFV *open*	BFV *close* when it should *open* & Previous state of BFV is *close*	H_6
	BFV *open* $\rightarrow$ BFV *close*	BFV *close* when it should *open* & Previous state of BFV is *open*	H_7
	BFV *open* $\not\rightarrow$ BFV *close*	BFV *open* when it should *close* & Previous state of BFV is *open*	H_8
FP	FP *on* $\rightarrow$ FP *off*	FP *off* when it should *on* & Previous state of FV is *on*	H_9
	FP *on* $\not\rightarrow$ FP *off*	FP *on* when it should *off* & Previous state of FV is *on*	H_{10}
	FP *off* $\rightarrow$ FP *on*	FP *on* when it should *off* & Previous state of FV is *off*	H_{11}
	FP *off* $\not\rightarrow$ FP *on*	FP *off* when it should *on* & Previous state of FV is *off*	H_{12}

TABLE 5.2: Hazards related to digital feedwater controller system

Hazard	Explanation
H_1	MFV *open* when it should *close* & FP *on* & Previous state of MFV is *close*
H_2	MFV *close* when it should *open* & FP *on* & Previous state of MFV is *close*
H_3	MFV *close* when it should *open* & FP *on* & Previous state of MFV is *open*
H_4	MFV *open* when it should *close* & FP *on* & Previous state of MFV is *open*
H_5	BFV *open* when it should *close* & FP *on* & Previous state of BFV is *close*
H_6	BFV *close* when it should *open* & FP *on* & Previous state of BFV is *close*
H_7	BFV *close* when it should *open* & FP *on* & Previous state of BFV is *open*
H_8	BFV *open* when it should *close* & FP *on* & Previous state of BFV is *open*
H_9	FP *off* when it should *on* & (MFP *open*$\cup$ BFP *open)* & Previous state of FP is *on*
H_{10}	FP *on* when it should *off* & (MFP *open* $\cup$ BFP *open)* & Previous state of FP is *on*
H_{11}	FP *on* when it should *off* & (MFP *open* $\cup$ BFP *open)* & Previous state of FP is *off*
H_{12}	FP *off* when it should *on* & (MFP *open* $\cup$ BFP *open)* Previous state of FP is *off*

system lead to catastrophic disaster. All hazards related to the digital feedwater controller system are shown in Table 5.2.

5.3.4 Phase 4: Map Failure Rate to All Identified Hazards Based on SIL (IEC 61508)

In this phase, we have list of all the identified hazards. Now, by use of SIL based on IEC 61508, we assigned required failure rate of each hazard on the basis of

TABLE 5.3: Highest SIL (IEC 61508) related to each Hazard

Hazard	Severity	SIL	Required Failure Rate h^{-1}	Parameter
H_1	L	1	$< 10^{-6}$	$\lambda_{0,1}$
H_2	H	4	$< 10^{-9}$	$\lambda_{0,2}$
H_3	H	4	$< 10^{-9}$	$\lambda_{0,3}$
H_4	L	1	$< 10^{-6}$	$\lambda_{0,4}$
H_5	L	1	$< 10^{-6}$	$\lambda_{0,5}$
H_6	H	4	$< 10^{-9}$	$\lambda_{0,6}$
H_7	H	4	$< 10^{-9}$	$\lambda_{0,7}$
H_8	L	1	$< 10^{-6}$	$\lambda_{0,8}$
H_9	H	4	$< 10^{-9}$	$\lambda_{0,9}$
H_{10}	L	1	$< 10^{-6}$	$\lambda_{0,10}$
H_{11}	L	1	$< 10^{-6}$	$\lambda_{0,11}$
H_{12}	H	4	$< 10^{-9}$	$\lambda_{0,12}$

severity of it. Table 5.3 shows highest failure rate related to each hazard and respective transition parameter (transition rate for which transition occurs from system working state to that specific hazardous state). So far, we have our state machine and its associated hazards with its failure rate (h^{-1}).

5.3.5 Phase 5: Expand State Machine with Failure Rate

To be able to estimate and model probability of hazards, those hazards have to expand the previously discussed state machines, describing the functionality of a system. One way of doing this is to use hierarchical state machines and introduce every hazard as a state. Then the state machine describing a system has one state called working mode and several failure mode states, i.e. each hazard would be a relevant failure mode state. In systems with parallel functions failures can

relate either to the existing hazards or combined to form a new hazard as a state. Since, several times it is possible that transition of system's state from lower to higher hazard. This illustrated in Figure 5.4 where, all the possible transitions are integrated with the state machine. In our case study, we ignore transitions between severities of hazards: 1) L $\rightarrow$ L and 2) H $\rightarrow$ L to avoid unnecessary computations.

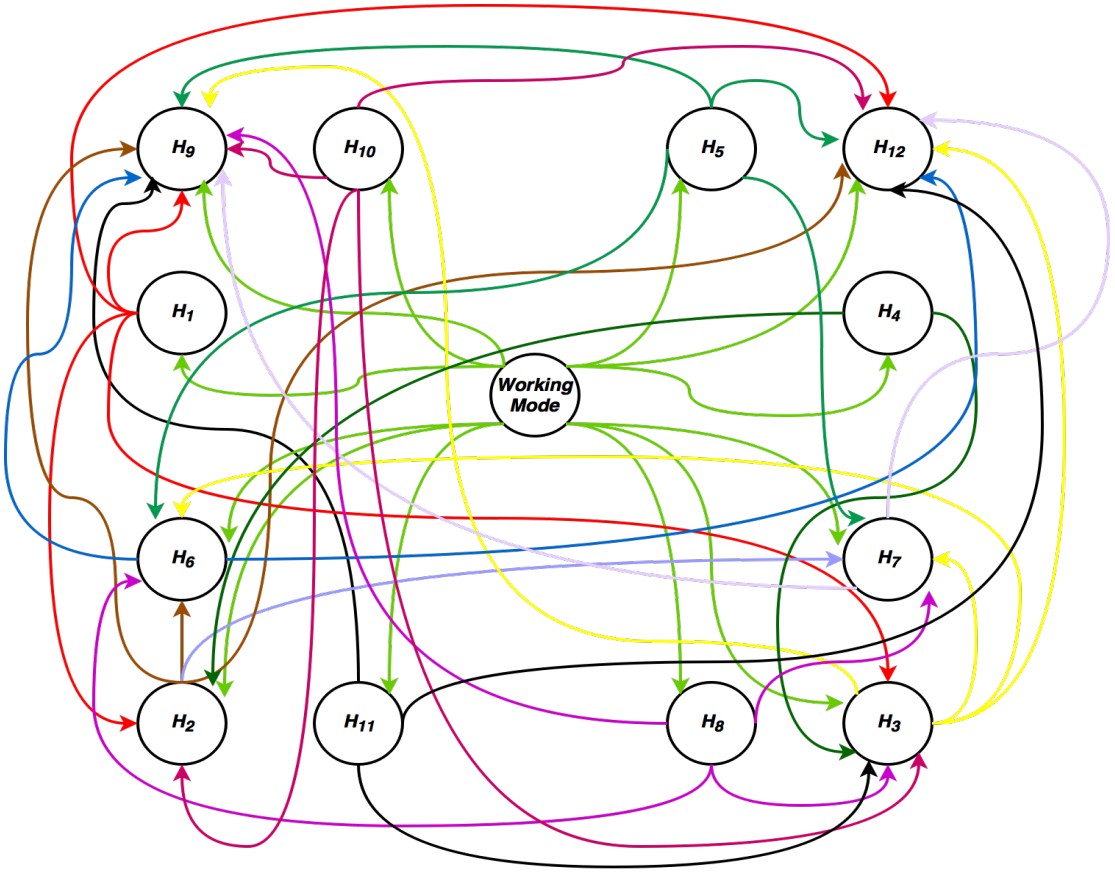

FIGURE 5.4: Expanded State Machine with working mode and failure rate

5.3.6 Phase 6: Convert the State Machine into CTMC Model and Assessment of Hazard Probability

State machine given in Figure 5.4 represents Markov model. In this phase, this Markov model is solved for the quantitative assessment of safety. The idea is to assign appropriate probabilities based on failure rates or SIL and then merge all state machines correctly making it possible to derive a transition probability matrix of the entire system. Using the required failure rates given in Table 5.3, the probabilities of the hazards can be computed. These probabilities give the likelihood of being in a specific hazard after 1 hour of system exposure. First of all, we have required deriving matrix P for the system. Since failure do not occur at specific time steps, but rather in a stochastic fashion, we use a CTMC. This matrix will then include the probability of being in a hazardous state, hence the probability of a hazard. This is

implemented in our case study as below.

$$P= \begin{bmatrix} 10^{-0}dt & \lambda_{0,1}dt & \lambda_{0,2}dt & \lambda_{0,3}dt & \lambda_{0,4}dt & \lambda_{0,5}dt & \lambda_{0,6}dt & \lambda_{0,7}dt & \lambda_{0,8}dt & \lambda_{0,9}dt & \lambda_{0,10}dt & \lambda_{0,11}dt & \lambda_{0,12}dt \\ 0 & 0 & \lambda_{1,2}dt & \lambda_{1,3}dt & 0 & 0 & 0 & 0 & 0 & \lambda_{1,9}dt & 0 & 0 & \lambda_{1,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & 2\lambda_{2,6}dt & 2\lambda_{2,7}dt & 0 & \lambda_{2,9}dt & 0 & 0 & \lambda_{2,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & 2\lambda_{3,6}dt & 2\lambda_{3,7}dt & 0 & \lambda_{3,9}dt & 0 & 0 & \lambda_{3,12}dt \\ 0 & 0 & \lambda_{4,2}dt & \lambda_{4,3}dt & 0 & 0 & 0 & 0 & 0 & \lambda_{4,9}dt & 0 & 0 & \lambda_{4,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{5,6}dt & \lambda_{5,7}dt & 0 & \lambda_{5,9}dt & 0 & 0 & \lambda_{5,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{6,9}dt & 0 & 0 & \lambda_{6,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{7,9}dt & 0 & 0 & \lambda_{7,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{8,6}dt & \lambda_{8,7}dt & 0 & \lambda_{8,9}dt & 0 & 0 & \lambda_{8,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{10,2}dt & \lambda_{10,3}dt & 0 & 0 & 0 & 0 & 0 & \lambda_{10,9}dt & 0 & 0 & \lambda_{10,12}dt \\ 0 & 0 & \lambda_{11,2}dt & \lambda_{11,3}dt & 0 & 0 & 0 & 0 & 0 & \lambda_{11,9}dt & 0 & 0 & \lambda_{11,12}dt \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Here, failure rates between two failure modes, for example, $\lambda_{i,j}(i < j \ or \ i > \ j)$ is the equivalent to direct failure rate from the Markov property, i.e.$\lambda_{i,j} = \lambda_{0,j}$. Using P matrix, the probability of each hazard can be computed as follows:

$$P_i(t) = \left(\frac{\lambda_{incoming\ edges}}{\lambda_{incoming\ edges} + \ \lambda_{outgoing\ edges}} \right) \times \left(1 - e^{-(\lambda_{incoming\ edges} + \ \lambda_{outgoing\ edges})t} \right) \tag{5.1}$$

Therefore, quantitative values of each hazard based on Equation 5.1 for t= 1 hour of the system exposure are:

$$
\begin{aligned}
P_1(H = H_1) &= 1.004301\times10^{-6} \\
P_2(H = H_2) &= 4.020133\times10^{-9} \\
P_3\,(H = H_3) &= 4.012123 \times 10^{-6} \\
P_4\,(H = H_4) &= 3.015101 \times 10^{-9} \\
P_5\,(H = H_5) &= 1.005033 \times 10^{-6} \\
P_6(H = H_6) &= 1.105536 \times10^{-8} \\
P_7(H = H_7) &= 2.010065 \times10^{-6} \\
P_8\,(H = H_8) &= 1.105537 \times10^{-8} \\
P_9\,(H = H_9) &= 1.012311 \times10^{-6} \\
P_{10}\,(H = H_{10}) &= 1.100555 \times10^{-8} \\
P_{11}\,(H = H_{11}) &= 1.100553 \times10^{-8} \\
P_{12}\,(H = H_{12}) &= 3.015097 \times10^{-6}
\end{aligned}
\tag{5.2}
$$

5.4 Experimental Validation

To validate the correctness of our approach and the accuracy of our results, we computed the failure rate of the same logic using the operational profile of three years. We developed a CBS, known as Test Facility, which is responsible to ensure the healthiness of all the DFWCS equipments, logics and interlocks. Test Facility is used to monitor the DFWCS process parameters round the clock and keeping in view of DFWCS below the target failure rate, it tests the DFWCS equipment once

in a month. Test Facility has a feature to log every action of the operator, every event and every changed state of any equipment or process parameters. During the testing, the conditions or logics are simulated and equipment operations, relevant to those conditions or logics are monitored and logged. For the control logic that we have taken as a case study, we took the log of the valve operation, as given in Table 5.4.

Calculating the failure rate for very small intervals, results in a hazard function or hazard rate $h(t)$ i.e.

$$\lim_{\Delta t \to 0} \frac{R\left(t\right) - R(t + \Delta t)}{\Delta t . R(t)}$$

Failure distribution $F(t)$ is a cumulative distribution function that describes probability of failure up to and including time t,

$$P\left(T \leq t\right) = F\left(t\right) = 1 - R\left(t\right), \quad t \geq 0$$

where T is the failure time. The failure distribution function of failure density function, $f(t)$ is given by

$$F\left(t\right) = \int_0^t f(\tau) d\tau$$

The hazard function is defined as:

$$h\left(t\right) = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)}$$

Since our model is the exponential failure distribution,

$$F\left(t\right) = \int_0^t \lambda e^{-\lambda\tau} d\tau = 1 - e^{-\lambda\tau}$$

$$\therefore h\left(t\right) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \tag{5.3}$$

Particularly for our case study, the entire input domain is partitioned into sub domains. Hence, we apply Brown and Lipow Input domain model [23] to compute the value ofλ. For this model, the operational profile must be specified as the probability, $P(E_i)$, that an input vector will be selected for each equivalence class. One must also have the number of test cases (or runs), n_i, from each equivalent class and the number, f_i, of those test cases that failed. It is assumed that no debugging occurs during testing. Reliability is estimated as:

$$\hat{R} = 1 - \sum_{i=1}^{M} \left(\frac{f_i}{n_i}\right) P(E_i) \tag{5.4}$$

The following seven steps were executed to compute the λ based on the operational profile data.

Step 1. Determine the operational profile

Step 2. Define the partition of the input of the input domain and assign operational probabilities to the equivalence classes in the partition

Step 3. Define failures

Step 4. Select a set of test cases for each equivalence class

Step 5. Run the tests

Step 6. Estimate the Reliability

Step 7. Estimate the hazard function λ.

Based on operational profile of 3 years, Table 5.4 presents the Input Domain Model calculation for DFWCS.

$$\therefore Total\ Estimated\ Reliability = 1 - \sum_{i=1}^{5} P(E_i)\left(\frac{f_i}{n_i}\right)$$

$$= 1 - 0.0466 = 0.9534$$

$$\because R(t) = e^{-\lambda t}$$

$$\therefore e^{-\lambda t} = 0.9534$$

$$\Longrightarrow \lambda = 1.81 \times 10^{-6}/hr$$

TABLE 5.4: Reliability Computation Using Brown and Lipow Model

Equivalence Class	$P(E_i)$	n_i	f_i	$P(E_i)\left(\frac{f_i}{n_i}\right)$
MFV State	0.10	20	1	0.0050
BFV State	0.10	20	1	0.0050
FP State	0.20	20	1	0.0300
MFV-FP State	0.05	30	1	0.0033
BFV-FP State	0.05	30	1	0.0033

From Equation 5.2, the hazard rate using our model is in the same order as computed using operational profile data. Hence, it proves the validity of our approach.

5.5 Conclusion

In present chapter, we proposed a framework for quantitative probabilistic hazard assessment (PHA) of the SCS and control system, with a case study of control system of NPP. Factually, the risk of safety norms violation leading to unsafe situation and hazardous state is modeled through quantitative PHA of the SCS and control system. From the present literature survey, there are qualitative and quantitative methodologies for safety analysis, based on different techniques such as Reliability Graphs, Event Tree Analysis, FTA, Generalized Stochastic Petri Nets and etcetera. In section 5.2, we conclude that in the existing frameworks, authors have assumed them either on the basis of some coarse knowledge or computed, using analytical methods which do not give accurate values. Some authors have quantified

hazards using operational profile but that is possible only after deployment of the system and hence it is not an early prediction. Our proposed framework is effective to overcome the limitations of existing methods and the validity of our approach has been demonstrated by 29 operational data sets of safety-critical systems. The application of our framework has been shown step-by-step on DFCW System in section 5.3.

In next chapter, an approach is proposed to remove system faults which are likely to get embedded because of ambiguous, inconsistent and incomplete requirements that leading to improper design and implementation, and the end result may be an unsafe system. It is the third contributory chapter.