International Journal of Engineering & Technology, 7 (2.12) (2018) 248-252

International Journal of Engineering & Technology

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

Research Paper

Early quantification of reliability for a safety critical and control system: a case study of reactor core cooling system

Vinay Kumar[1] *, Suraj Gupta [1], Anil Kumar Tripathi [1]

[1] *Indian Institute of Technology (BHU), Varanasi, India*
**Corresponding author E-mail: vk841232@gmail.com*

Abstract

Using Probabilistic Reliability analysis for Quantifying reliability of a system is already a common practice in Reliability Engineering community. This method plays an important role in analyzing reliability of nuclear plants and its various components. In Nuclear Power Plants Reactor Core Cooling System is a component of prime importance as its breakdown can disrupt Cooling System of power plant. In this paper, we present a framework for early quantification of Reliability and illustrated with a Safety Critical and Control System as case study which runs in a Nuclear Power Plant.

Keywords: *Fault Tree; Nuclear Power Plan; Reliability Analysis Technique; Reliability Block Diagram; Safety Critical and Control System.*

1. Introduction

Safety Critical and Control Systems [1-3] are those systems whose failure may lead to mission loss, significant financial loss, damage to environment, or even cause to severe injuries or deaths. Therefore, it is very important that SCCS should be reliable to gain in confidence of user(s) for its use and Reliability engineering assures that a SCCS works properly for a given period of time. Reliability of a system is the probability such that given system works properly with its components for a given period of time.

As failure of SCCS is very high, therefore, it is good to estimate reliability of a system during design and architectural phase of system development life cycle prior to actual deployment of the system. There are many reliability techniques are available for such purposes which gives a qualitative or quantitative overview for a SCCS and can be utilized to know at "what extent of our designed system is reliable." The early quantification of reliability [4] of a SCCS can help to choose better design, good maintenance policies, lower cost estimation for failure, and maximum warranty period of the product. But, most of the available methods are probabilistic in nature, therefore, in this present paper we propose a hybrid model which is based on various Reliability analysis techniques for early quantification of a SCCS with more accuracy.

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

2. Background details and related work

Reliability Block Diagram Method [5] - In Reliability block diagram, components of system are represented as blocks and joined in order of their functioning in the system. Systems can be configured in many ways out of which some are parallel configuration, series configuration, complex configuration, N-out-of-K system, and standby redundant systems.

M. C. Kim [6] proposed a method for a reliability analysis by use of reliability graph and general gates (RGGG). However, the case study used is very simple.

Cheng-Min Lin et al. [7] proposed an approach based on reliability block diagram for Reliability analysis of mesh network. However, the case study used to illustrate the approach is not a real-world example.

Fault Tree Method [8] – In fault tree method, the reliability of system is quantified using failure of its components. The failure of each component may or may not affect the overall working of system.

Bing Wang et al. [9] developed a reliability model for electric vehicle motor by using fault tree. However, authors did not validate this method using actual reliability test data.

Success Tree Method [10] – This method is similar to the fault tree method but instead of failures of components, their success is taken into account.

Event Tree Method [11] – All possibilities of failures and success of each component is used to determine all possible sequences and result of each sequence is shown at its end. This result denotes whether system will succeed or fail with this possible sequence.

3. Proposed approach

Probabilistic Reliability Analysis (PRA) is currently being widely applied to many fields. PRA is being used all over the world in nuclear facilities, aerospace, the chemical and process plants, and these days, even in the field of financial management. The aim of PRA is to evaluate the failure rate of the components and the combination(s) of these failures of components which can lead to failure of a whole system, assessing each combination and its probability of occurrence and evaluation of the reliability of a system. As PRA

estimate Reliability quantitatively, which can be useful for comparing alternatives in different engineering and design areas.
In spite of the benefits, PRA has its own well-known restrictions. Uncertainties in characteristics like data and models and human reliability effect the precision of the PRA. Therefore, we proposed a framework for the early quantification of Reliability based on hybrid modelling. The framework is shown in Fig. 1.

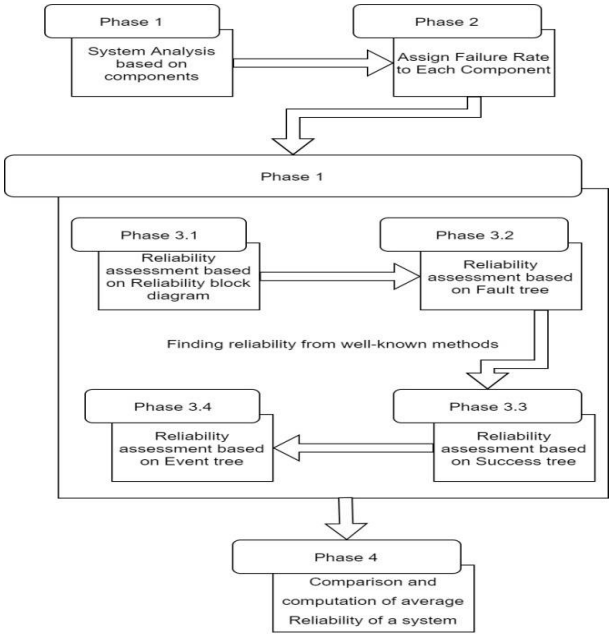

Fig. 1: A Framework for Early Quantification of Reliability Experimental Setup and Results.

4. Experimental setup and results

A Case Study: Reactor Core Cooling System (RCCS)
ET1: Water tank used for holding coolant,
SV1-SV7: Motor operated valves,
SP1-SP2: Water Pumps,
SN1-SN2: Spray Nozzles,

4.1. RCCS overview

The RCCS is a complex configured system whose objective is to supply coolant to the reactor in case of need. Fig. 2 shows the structure of a general RCCS. The coolant is supplied from tank containing it to the reactor through several pumps and valves. Coolant is supplied from either of spray nozzles. It prevents the problems caused due to overheating of reactor.
The RCCS is composed of water tank, two water pumps, seven motor operated valves, and two spray nozzles.
The system coolant is supplied to the reactor through either of spray nozzles. It is passed from water tank to reactor through several valves and pumps. If any path of water supply fails then the system relies on the alternative path. Also motor operated valve SV5 ensures optimal operability of system through crossed paths.

4.2. RCCS operation

RCCS is used in two situations. These are termed as long-term and short-term missions depending on the plant requirement durations of need of coolant. These two operational missions differ in the time the system was operated for the particular event of cooling purpose. Those missions which require the use of RCCS coolant supply for less than fifteen minutes are termed as short-term missions. That means short-term missions aim the operation of RCCS's coolant supply for only a few minutes duration. Other missions where supply of coolant is needed for more than fifteen minutes are termed as long-term missions. A long-term mission may require the operation of a RCCS system for several hours.

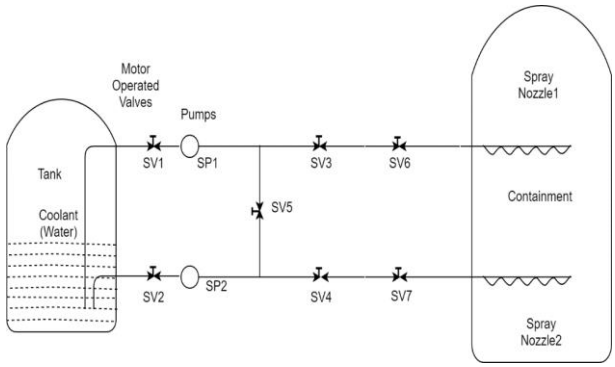

Fig. 2: A schematic diagram of RCCS

4.3. Different phases of proposed framework

Phase 1: System analysis based on components
In this phase, system is analyzed for the components used in the system and whose coordinated functioning is required for proper goal of whole system. All the components of RCCS are listed under Table 1.

Table 1: Components Used in RCCS

Component
SV1: Valve1
SV2:Valve2
SP1:Pump1
SP2:Pump2
SV3:Valve3
SV4:Valve4
SV5:Valve5
SV6:Valve6
SV7:Valve7
SN1:SprayNozzle1
SN2:SprayNozzle2

Phase 2: Assign failure rate to each component
In this phase, failure rate of each component is collected from operational profile of a system. Table 2 shows the failure rate of all the components of RCCS and its reliability for one hour based on 3 years of operational profile data of Nuclear Power Plant.

Table 2: Failure Rate (h^{-1}) of Each Component

Component	Failure Rate	Reliability
Valve1	5x10-3	0.995
Valve2	5x10-3	0.995
Pump1	4x10-3	0.996
Pump2	4x10-3	0.996
Valve3	8x10-3	0.992
Valve4	8x10-3	0.992
Valve5	7x10-3	0.993
Valve6	9x10-3	0.991
Valve7	9x10-3	0.991
Nozzle Spray1	6x10-3	0.994
Nozzle Spray2	6x10-3	0.994

Phase 3: Finding reliability from well-known methods
In this phase, Reliability of system is found from different methods which are following:
Phase 3.1: Reliability assessment based on reliability block diagram
Reliability block diagram of a given system often corresponds to the physical arrangement of components in the system. For given RCCS, Reliability block diagram is prepared and then reliability is calculated as shown in Fig. 3 by using given two equations. For series and parallel configuration of components respectively:
For Series configuration:

$$R(t) = \mathbb{\Pi}_{i=1}^{n} R_i(t) \quad (1)$$

And for Parallel configuration:

$$R(t) = 1 - \mathbb{I}\mathbb{I}_{i=1}^{n}(1 - R_i(t)) \quad (2)$$

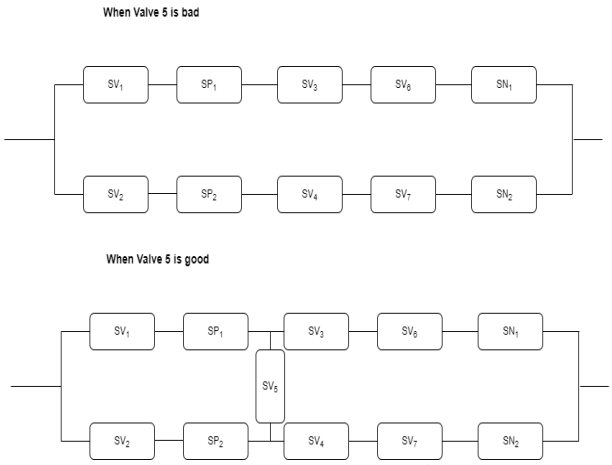

Fig. 3: Reliability Block Diagram of RCCS.

Reliability of first series combination
= 0.995 x 0.996 x 0.992 x 0.991 x 0.994
= 0.968.
Reliability of second series combination
= 0.995 x 0.996 x 0.992 x 0.991 x 0.994
= 0.968.
Reliability of parallel combination of these two
= 1 – (1-0.968) x (1-0.968)
= 0.998

Phase 3.2: Reliability Assessment based on Fault Tree

The fault tree method is a deductive approach for quantification of reliability. The failure of system is the top event in the fault tree and possible causes of each event is shown below. For RCCS, the fault tree constructed is shown in Fig. 4.

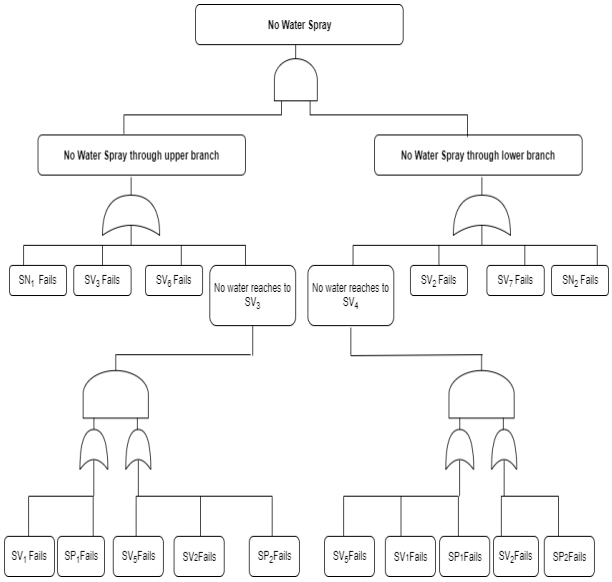

Fig. 1.4: A Fault Tree for RCCS.

Using failure rate to compute reliability we get

$$R(t) = 1 - F(t) \quad (3)$$

Also, AND key works like intersection and OR key works like union and we know that

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \quad (4)$$

And also for two exclusive sets A and B

$$P(A \cap B) = P(A).P(B) \quad (5)$$

So, this gives us system's reliability = 0.999

Phase 3.3: Reliability Assessment based on success tree method

The success tree method is also a deductive approach for reliability quantification. Success and fault trees are logical complements of each other. The events of failure in fault tree are events of success in success tree. Top event is the success of the system, which downwards tells the requirements of successful operation of components contributing. Success Tree for RCCS is shown in Fig. 5.

Success tree and fault tree are logically complementary of each other. AND keys get converted in OR keys and vice-versa.

Calculating reliability of given system with above success tree we get,

Reliability = 0.999.

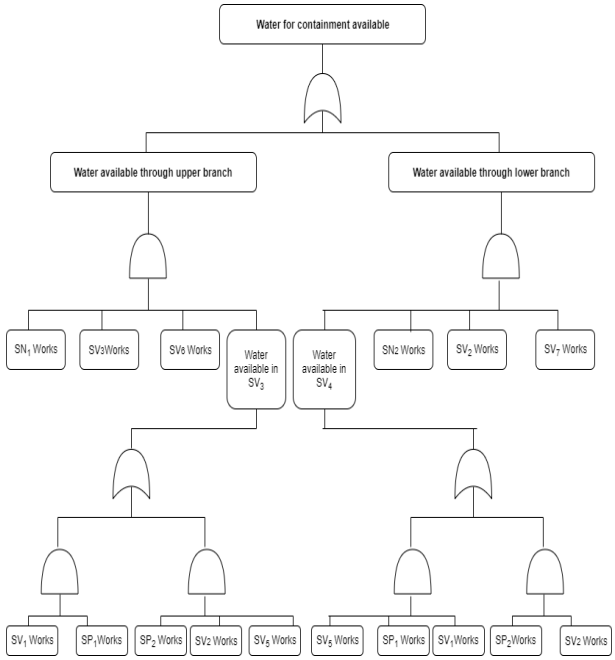

Fig. 1.5: A Success Tree for RCCS.

Phase 3.4: Reliability assessment based on event tree

Event tree follows a binary format that means the event at heading is assumed to either occur or not occur. This results in several possible sequences of components operational status. Each sequence either results in overall system success or failure shown in Fig. 6 and Fig. 7.

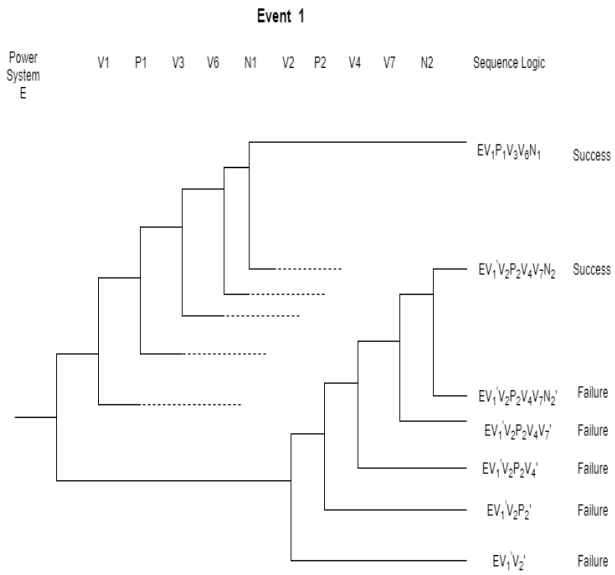

Fig. 1.6: An Event Tree of RCCS for Event 1.

In event trees those sequences which result in success of overall system contribute in quantification of reliabilities. In given event trees, such sequences are shown in Table 3.

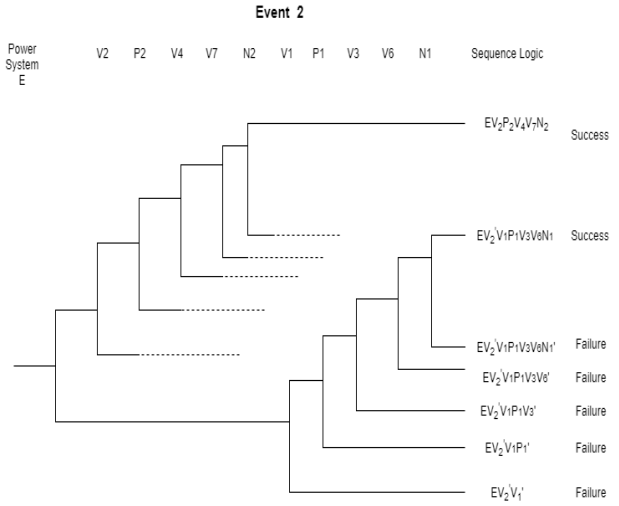

Fig. 1.7: An Event Tree of RCCS for Event 2.

Table 3: Probabilities of Different Sequences

Sequence	Probability
$EV_1P_1V_3V_6N_1$	0.968
$EV_1P_1V_3V_6N_1$' $V_2P_2V_4V_7N_2$	0.005
$EV_1P_1V_3V_6$' $V_2P_2V_4V_7N_2$	0.008
$EV_1P_1V_3$' $V_2P_2V_4V_7N_2$	0.007
EV_1P_1' $V_2P_2V_4V_7N_2$	0.004
EV_1' $V_2P_2V_4V_7N_2$	0.004
$EV_2P_2V_4V_7N_2$	0.968
$EV_2P_2V_4V_7N_2$'$V_1P_1V_3V_6N_1$	0.005
$EV_2P_2V_4V_7$'$V_1P_1V_3V_6N_1$	0.008
$EV_2P_2V_4$'$V_1P_1V_3V_6N_1$	0.007
EV_2P_2'$V_1P_1V_3V_6N_1$	0.004
EV_2'$V_1P_1V_3V_6N_1$	0.004

Hence total reliability of given system
=
(0.968+0.005+0.008+0.007+0.004+0.004+0.968+0.005+0.008+0.007+0.004+0.004) / 2
= 0.996.

Phase 4: Comparison and computation of average reliability of a system

Reliabilities obtained from different methods used are not exactly same in the value. It is also difficult to say which of these methods is best for computing reliabilities of systems.

We can see from average of all these results that which of these methods is fit for this type of systems. Average reliability is computed from following formula:

$$R_{avg}(t) = \frac{\sum_{i=1}^{N} R_i(t)}{N} \; ; \forall \; i \; \epsilon \; \{0, 1, 2, 3, 4\} \tag{6}$$

Table 4 represents obtained results of our system for different established methods.

Table 4: Estimated Reliability Based on Various Methods

Method	Reliability
RBD	0.998
Fault Tree	0.999
Success Tree	0.999
Event Tree	0.996

Comparison of the obtained results is shown in Fig. 8.

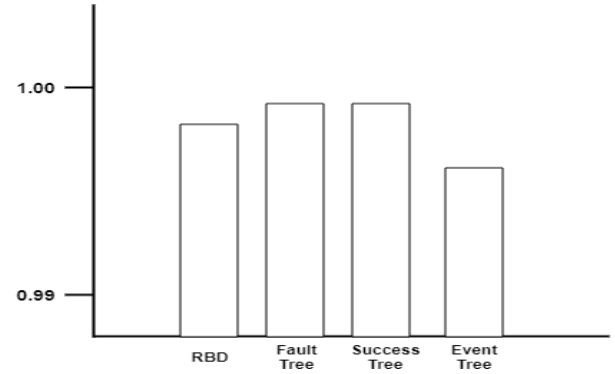

Fig. 8: Comparison among All the Estimated Reliability Using Various Methods.

So, Average reliability

$$= (0.998 + 0.999 + 0.999 + 0.996)/4$$

= 0.998

From the operational profile data of 3 years, the computed reliability [12] of the safety critical system given by

$$R_{actual} = 0.99484$$

Now comparing the predicted and computed reliability figure, the predicted reliability $R_{predicted}$ is slightly greater than the computed reliability R_{actual} , with the difference given by $R_{difference}$:

$$R_{predicted} > R_{actual}$$

$$R_{difference} = R_{predicted} - R_{actual} \tag{7}$$

= 0.998 – 0.99484

= 0.00316

Thus, after computing the reliability of our safety critical system, we obtain a prediction accuracy of 99.684 percent. Hence, it proves the validity of our methodology.

5. Conclusions

Reliability approaches have been intensively studied in past decades. This results in many research papers based on reliability 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 reliability of a safety critical system based on hybrid model. This frame utilizes features of RBD Technique, Fault tree, Success 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 RCCS. The result of the proposed approach shows its effectiveness.

References

[1] 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, (2017), pp. 38-47.

[2] 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.

[3] 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.

[4] 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.

[5] Čepin Marko, "Reliability block diagram." In Assessment of Power System Reliability, Springer London, (2011), pp. 119-123.

[6] Kim M. C., "Reliability block diagram with general gates and its application to system reliability analysis." *Annals of Nuclear Energy* 38, no. 11, (2011), pp. 2456-2461.

[7] Lin Cheng-Min, Teng Hui-Kang, Yang Cheng-Chih, Weng Hwei-Li, Chung Ming-Cheng, and Chung Chiu-Chiao, "A mesh network reliability analysis using reliability block diagram," In Industrial Informatics (INDIN), 8th IEEE International Conference, (2010) , pp. 975-979.

[8] Ericson Clifton A., "Fault tree analysis." In System Safety Conference, Orlando, Florida, (1999), pp. 1-9.

[9] Wang Bing, Tian Guangdong, Liang Yanping, Qiang Tiangang. "Reliability modeling and evaluation of electric vehicle motor by using fault tree and extended stochastic Petri nets," *Journal of Applied Mathematics*, Volume 2014, (2014), pp. 1-9.

[10] Ireson William Gran, Coombs Clyde F., and Moss Richard Y. Handbook of reliability engineering and management. McGraw-Hill Professional, (1996).

[11] Raiyan Asif, Das Subir, and Islam M. Rafiqul. "Event Tree Analysis of Marine Accidents in Bangladesh." Procedia Engineering 194, (2017), pp. 276-283.

[12] Singh, Lalit Kumar,Vinod Gopika, and Tripathi Anil Kumar. "Early prediction of software reliability: A case study with a nuclear power plant system." *Computer* 49, no. 1, (2016), pp. 52-58.