

Reliability Analysis of Core Protection Calculator System using Petri Net

Hyejin Kim^{*a}, Jonghyun Kim^b

^a KEPCO Nuclear Fuel, Daejeon-si, Korea

^b KEPCO International Nuclear Graduate School, Ulsan-si, Korea

Abstract: As digital systems are introduced to nuclear power plants, issues related with reliability analyses of these digital systems are being raised. One of these issues is that static Fault Tree (FT) and Event Tree (ET) approach cannot properly account for dynamic interactions in the digital systems, such as multiple top events, logic loops and time delay. This study proposes an approach to analyzing the reliability of Core Protection Calculator System (CPCS) using Petri Net (PN) modeling. The PN, one of the dynamic methodologies, allows modeling event dependencies and interaction to represent the time sequence and delay time for dynamic events. This study applies the approach to the reliability analysis of CPCS. In order to analyze the digital system modeling, further studies are required with the dynamic modeling methods and the software in the digital system. Modeling of digital systems should be realistic to account for the system characteristics and be able to predict system behavior.

Keywords: Dynamic PSA, Petri Net, CPCS.

1. INTRODUCTION

Digital technology is replacing the analog Instrumentation and Control (I&C) systems in both new and upgraded nuclear power plants. As digital systems are introduced to nuclear power plants, issues related with reliability analyses of these digital systems are being raised. One of these issues is that static FT and ET approach cannot properly account for dynamic interactions in the digital systems, such as multiple top events, logic loops and time delay [1].

Given the limitations of static modeling methods when applied to dynamic systems, several studies on dynamic modeling methods have been conducted. Most research has involved existing modeling methods in order to integrate easily with static methods, which have already been widely implemented in the system modeling field. Some of dynamic methods have been upgraded making it possible to analyze the dynamic interactions between components of dynamic systems [2].

The presence of the interaction among complex hardware, software and physical processes in digital I&C systems may necessitate the use of dynamic methodologies for dependable results. Dynamic methodologies are defined as those that can account for the coupling between the triggered or stochastic logical events in system reliability modeling, through explicit consideration of the time element in system evolution. Many methods have been proposed to solve the problems, but there is no single method that is universally accepted for the application to the current generation Probabilistic Safety Analysis (PSA)[3].

On the other hand, some assumptions are used to analyze the reliability of Reactor Protection System (RPS), which is one of the digital I&C system, there is no consideration except for ex-core signal as an input for Core Protection Calculator System (CPCS) to avoid the complexity for modeling the RPS system in Shin-kori 3&4 PSA Report [4]. CPCS is a digital computer system which continuously calculates Departure from Nucleate Boiling Ratio (DNBR) and Linear Power Density (LPD) to initiate a reactor trip when needed during certain transients to prevent violation of the DNB and LPD safety limits.

In this study, PN is extended to model system failures. PN method for qualitative and quantitative

^{*} Corresponding author : heyjin@knfc.co.kr

analysis of CPCS in Advanced Power Reactor 1400 (APR1400) is presented.

2. PN MODELING METHOD





The PN, one of the dynamic methodologies, allows modelling the event dependencies and interaction, to represent the time sequence and delay time, and to model assumptions for dynamic events [5].

The PN is a directed graph consisting of two types of nodes, called places and transitions. Systems are modeled as a set of conditions and events. Places represent conditions in the process, and transitions represent events. Transitions can be immediate, deterministically time-delayed, or time-delayed based on a probability distribution defined by the user [5]. Also, the PN model allows explicit representation of the time elements of system with the use of a dynamic system model and subsequently is capable of simulation of concurrent and dynamic activities and time-delays [6].

Events such as ‘transmitter fails’ are represented by nodes. Arcs connect either transitions to nodes or nodes to transitions. It uses tokens that can move when the PN is executed for the representation information flow through the net. A token moves from a node or place and is consumed by a transition. When a transition fires, it produces tokens in places that it connects to and consumes one token in each of the places that connect to it. In order for a transition to fire it must have at least one token on each of its input places. Transition delays and timed transitions can be represented [6]. The state of a net is modeled by the presence or absence of a token in the places. An event occurs only when the preconditions are met and is represented by an enabled transition. The firing of a transition changes the marking of its input and output places, modeling a change in its precondition and post-conditions.

PN consists of four basic elements [4] as stated in Table 1:

Table 1: Basic Elements of PN

Figure	Name of element	Drawn as	denotation
	Place	Circle	Event
	Transition	Cube or Bar	Event transfer
	Arc	Arrow	Transfer between places and transitions
	Token	Dot	Data

Places indicate failures, transition expresses the event transfer and delay time, and token indicates the condition of failure in the PN modeling in this study.

3. CASE STUDIES: RELIABILITY ANALYSIS OF CPCS

3.1 CPCS Design Basis [7]

The CPC design basis requires that the system calculate conservative, but relatively accurate, values of Departure from Nucleate Boiling Ratio (DNBR) and Local Power Density (LPD). In order to achieve a system time response sufficient to accommodate the limiting design basis events, additional dynamic calculations of DNBR and LPD are required. The dynamic calculations must provide conservative estimates of DNBR and peak linear heat rate based on changes in the process variables between successive detailed calculations of DNBR and LPD.

The resultant protection software consists of six interdependent programs, five of which are resident in the CPC processor, and the sixth in each Control Element Assembly Calculator (CEAC) processor:

- Coolant Mass Flow Program (FLOW)
- DNBR and Power Density Update Program (UPDATE)
- Power Distribution Program (POWER)
- Static DNBR and Power Density Program (STATIC)
- Trip Sequence Program (TRIPSEQ)
- CEAC Penalty Factor (PF) Program (CEAC).

In the CPCS, the TRIPSEQ Program shall compare the DNBR and LPD to their respective pretrip and trip setpoints. Whenever a setpoint is violated, the appropriate contact output is actuated.

Figure 1 shows the CPCS Algorithm Diagram among the six programs.

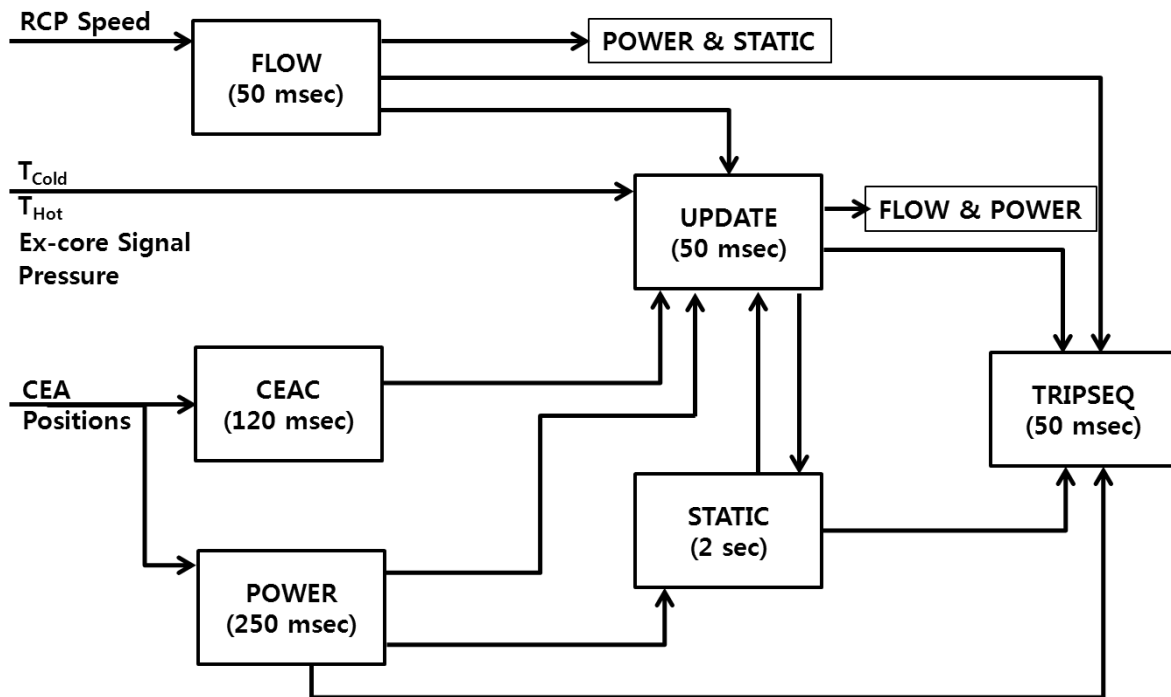


Figure 1: CPCS Algorithm Diagram

3.2 PN Modeling

This paper applies the proposed approach to analyzing the reliability of CPCS. More specifically, the scope of modeling is processing the pressurizer pressure signal for generating the DNBR trip signal to Plant Protection System (PPS). PN modeling includes the transmitter, converter, analog input card module, processing module, and contact to PPS. Continuously repeated execution is expressed using the place 'E' and arc 'e'. Some of the delay times are expressed as 'DT1' and 'DT2' for convenience in Figure 2.

Figure 2 shows the PN to represent the failure of trip signals to PPS from pressurizer pressure transmitter for pressurizer pressure signals. The transmitter senses the pressure inputs and transforms it to the current signal. The I/E converter transforms the signal from current to voltage. The AI685 analog input card module continuously scans, stores, and transforms the analog input to digital values.

The UPDATE program reads the digital values from the AI685 and calculates the DNBR, and the TRIPSEQ program compares the DNBR to its setpoint values. If the DNBR is lower than the setpoint, a trip signal is generated.

Figure 2 include: 1) the time sequence from pressurizer pressure transmitter to contact to PPS, 2) the interaction between hardware and software, 3) the time-delay to process the input signals, e.g. T5 and T7, 4) the continuous scanning and memory update, e.g. P8, and 5) the execution of processing modules, e.g. P7.

This modeling was done by using the Colored PN Ver. 4.0. [8].

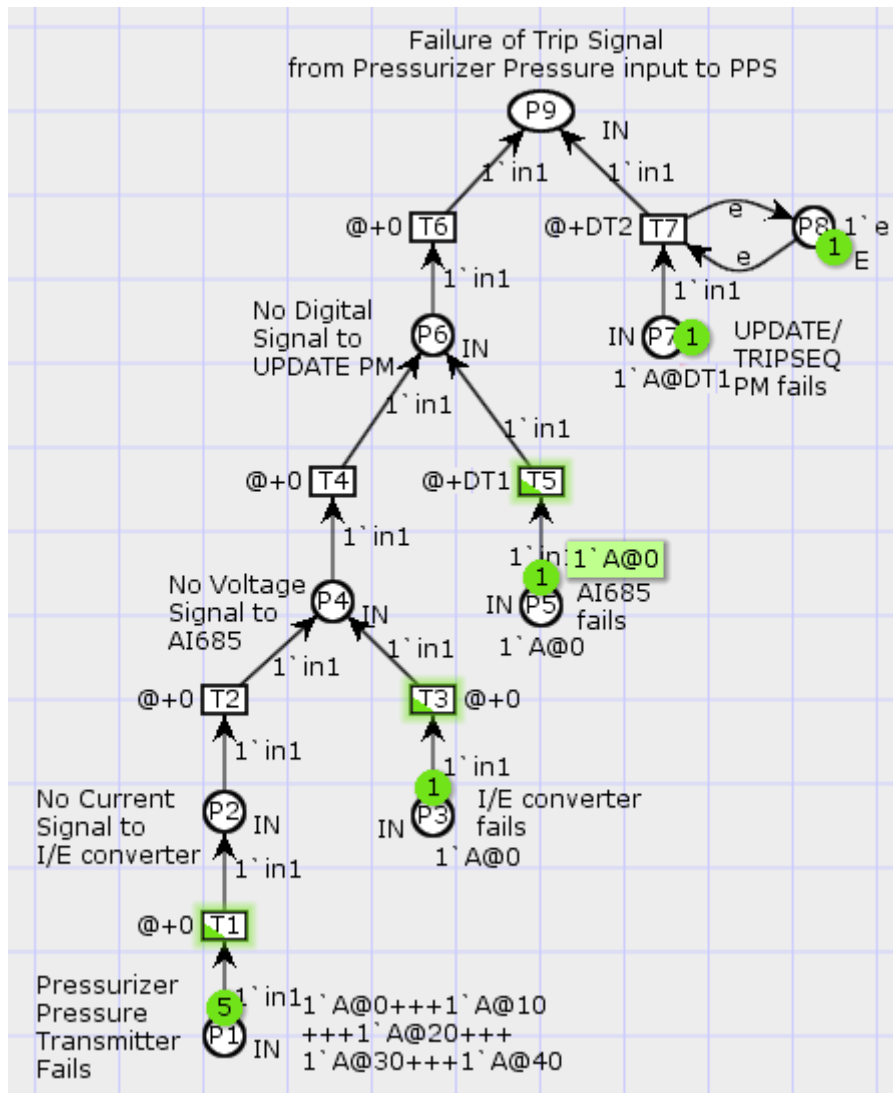


Figure 2: PN modeling for Pressurizer Pressure signal

3.3 Interaction

The presence of the interaction among complex hardware, software and physical processes in digital I&C systems may necessitate the use of dynamic methodologies for dependable results. The PN allows modeling event dependencies and interaction to represent the time sequence and delay time for dynamic events.

Figure 3 represents the interaction among Hardware/Software/Processing modules in CPCS. The interaction 1) between hardware, e.g. P1, P2, P3, P4, P5 and P6, and software, e.g. P16, and 2) among the processing modules, e.g. P11, P13, P15, P16, P19, and P20, are presented.

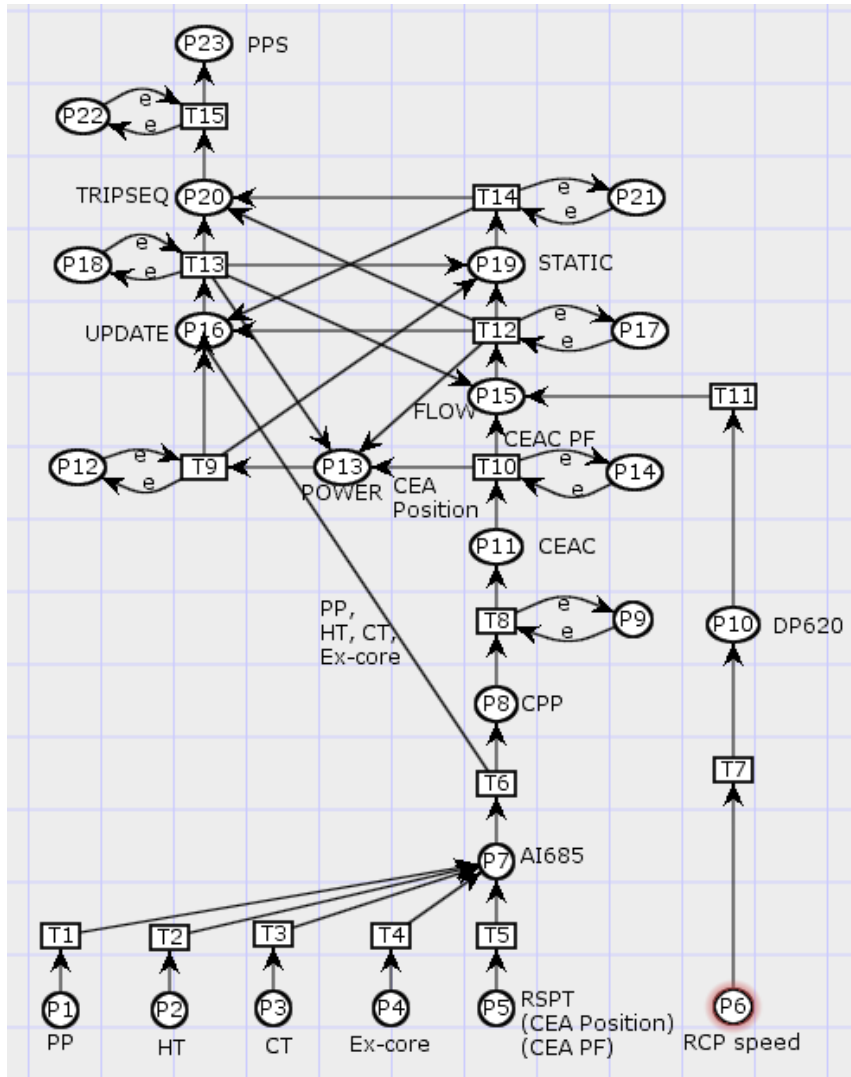


Figure 3: Interaction among Hardware/Software/Processing module in CPCS

3.4 PN Quantification

3.4.1 Failure Probability Calculation

As long as the failure probability of basic events in a fault tree is given, the reliability or failure probability of the top event can be calculated. It is known that calculating failure probability for a fault tree depends on gates. However, for PN it depends on symbols of transitions, places and arcs [9].

The failure probability P_f in case of a transition with multi-input places can be written as:

$$P_f = \prod_{i=1}^n P_{fi} \quad (1)$$

where, P_{fi} denotes the failure probability of the i_{th} event.

By contrast, the failure probability for a place with multi-input transitions is written as:

$$P_f = 1 - \prod_{i=1}^n (1 - P_{fi}) \quad (2)$$

It is not necessary to calculate for the transition or place with single input.

3.3.2 Minimal Cut Set – Matrix Method

Minimal cut sets can be found at the same time using the present matrix method to analyze the PN from a top place to basic places. This method proceeds as follows [9]:

1. Write down the numbers of places by making a horizontal arrangement if the output place is connected by multi-arcs to transitions.
2. Write down the numbers of places by making a vertical arrangement if the output place is connected by an arc to a common transition.
3. When all places are replaced by basic places, a matrix is established. If there is common entry located between rows or columns, it is the entry shared for each row or column, the column vectors of the matrix represent cut sets.
4. Remove the supersets to obtain the minimal cut sets.

From the PN modeling, cutsets and failure probability are calculated using the matrix methods [9].

Figure 4 gives minimal cutsets for the PN depicted in Figure 2. Consequently, minimal cut sets are [P1], [P3], [P5], and [P7] and they are obtained by using matrix method.

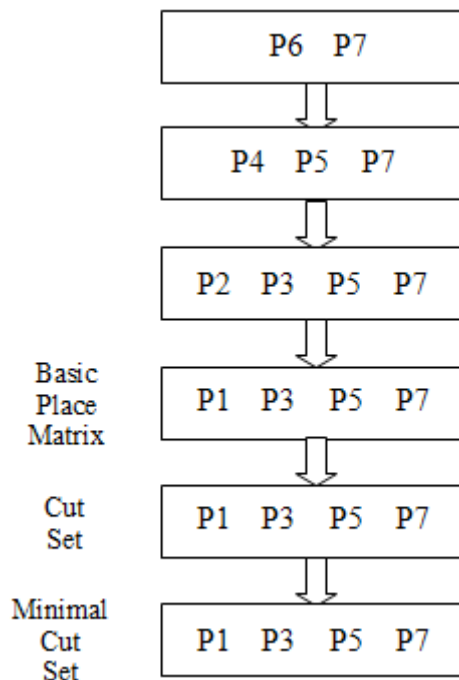


Figure 4: Matrix method for Pressurizer Pressure Input

The failure probability for a place with multi-input transitions is written as:

$$P_f = 1 - \prod_{i=1}^n (1 - P_{fi}) = 1 - (1 - P1)(1 - P3)(1 - P5)(1 - P7) \quad (3)$$

Using the methods mentioned above, failure probability for CPCS is calculated. Some failure probability data are used as it is in Shin-kori 3&4 PSA Report [4] and some are assumed. Software failure probability is assumed that the contribution from software failure to total failure probability is 10% of the hardware failure probabilities [10].

Following the failure probability data and equations, failure probability for the “Failure of Trip Signal (DNBR) from CPCS input signals to PPS is calculated as $3.73605E-3$.

4. CONCLUSION

Until a recent date, static modelling, e.g. FT and ET, are extensively used in PSA to model and evaluate the probability and consequence of failures of nuclear power plants. Given the limitations of static modeling methods when applied to dynamic systems, several studies on dynamic modeling methods have been conducted.

To overcome the limitations of static modeling methodologies for the digital system, this study proposes an approach to analyzing the reliability of CPCS using PN method. Both qualitative, e.g. PN modelling, and quantitative, e.g. failure probability calculation, analyses for CPCS in APR1400 are presented. Failure probability and minimal cutset are also presented from the PN modeling by using the equation and matrix method.

In order to analyze the digital system modeling, further studies are required with the dynamic modeling methods. In addition, the study on the software in the digital system are also recommended to consider the precise failure probability, common cause failure, human error, software HAZOP (Hazard and Operability) results, and Failure Mode Effect Analysis (FMEA) for the reliability analysis. Modeling of digital systems should be realistic to account for the system characteristics and be able to predict system behavior.

References

- [1] US NRC, “Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments”, NUREG/CR-6942, (2000).
- [2] Shin, S.K. and Seong, P.H., “Review of various dynamic modeling methods and development of an intuitive modeling method for dynamic systems”, Nuclear Engineering and Technology, Vol. 40, No.5, (2008).
- [3] Lu, L, “An Overview of Digital I&C System Reliability Analysis in Nuclear Power Plants”, NPIC&HMIT, Albuquerque, (2006).
- [4] KHNP, “Shin Kori 3&4 Probabilistic Safety Assessment (PSA) report”, (2011).
- [5] Lee, A and Lu, L, “Petri Net Modeling for Probabilistic Safety Assessment and its application in the air lock system of a CANDU nuclear power plant”, Procedia Engineering, Vol. 45, pp11 – 20, (2012).
- [6] US NRC, “Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments”, NUREG/CR-6901, (2006).
- [7] KEPCO Nuclear Fuel, “Functional Design Requirements for a Core Protection Calculator System for Shinkori Nuclear Power Plant Units 3&4”, (2010).
- [8] Coloured Petri Net, Version 4.0. <http://cpntools.org/>.
- [9] Liu, T.S. and Chiou, S.B, “The Application of Petri Nets to Failure Analysis”, Reliability Engineering and System Safety, Vol. 57, pp. 129-142, (1997).

[10] Authen, S. and Holmberg, J. E, "Reliability Analysis of Digital Systems in a Probabilistic Risk Analysis for Nuclear Power Plants", Nuclear Engineering and Technology, Vol. 44, No.5, (2012).