Reliability Analysis of Core Protection Calculator System by Combining Petri Net and Fault Tree

*Hyejin Kim, Jonghyun Kim,
KEPCO International Nuclear Graduate School, 1456-1 Shinam-Ri, Seosaeng-Myeon, Ulju-Gun, Ulsan
**Corresponding author: liberty622@nate.com*

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 [1].

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 [1]. 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) [2].

This paper proposes an approach to analyzing the reliability of digital systems by combining Petri net (PN) and Fault tree. The Petri net allows modeling event dependencies and interaction, to represent the time sequence, and to model assumptions for dynamic events. The Petri net model can be straightforwardly transformed to fault tree using the gate. Then, the FT can be integrated into the existing PSA. This paper applies the approach to the reliability analysis of Core Protection Calculator System (CPCS).

2. Petri Net Modeling

2.1 Petri Net

The Petri net 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. 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 [3].

Petri nets consist of four basic elements: places, transitions, tokens and arcs:

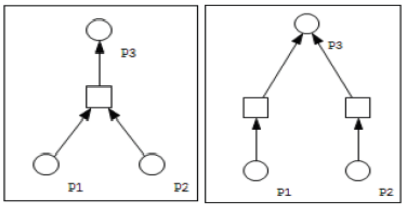
⬭ : Place, drawn as a circle, denotes event
□ : Transition, drawn as a bar/cube, denotes event transfer
→ : Arc, drawn as an arrow, between places and transitions
● : Token, drawn as a dot, contained in places, denotes the data

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

2.2 Transformation from Petri Net to Fault Tree

The Petri net can be directly transformed into fault trees. Figure 1 shows the Petri net models which are corresponding to AND and OR gates of fault tree. In Fig. 1 (a), Place P3 has a token when Places P1 and P2 have a token simultaneously. This is correspondent to an AND gate. In Fig. 1 (b), Place P3 has a token when either P1 or P2 has a token. This is the same logic as OR gate.

To analyze the reliability of digital systems, this paper proposes two-step approach: 1) modeling the failure by using the Petri net and 2) transforming the Petri net model into a fault tree model.



(a) (b)

Fig. 1. Gate representation in Petri net (a) AND gate, and (b) OR gate [3]

3. Case Study: Reliability Analysis of CPCS

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 and LPD Trip signal to Plant Protection System (PPS). It includes the transmitter, I/E converter, AI685 analog input card, UPDATE/TRIPSEQ program processing, interposing relay, and the contact to PPS. Transmitter senses the pressurizer pressure inputs and transforms it to the current signal. I/E Converter transforms the signal from currents to voltages. The AI685 analog input card continuously scans, stores values and transforms analog input to digital values. The UPDATE program reads the digital values from AI685 and calculates the DNBR and LPD, and TRIPSEQ program compares the DNBR and

LPD to setpoint values. If DNBR is lower or LPD is higher than setpoint values, trip signal will be generated, and in turn de-energize an interposing relay, which provides open trip contacts to the PPS.

Fig. 3 shows the Petri net to represent the failure of trip signals to PPS from transmitter for pressurizer pressure signals. It includes: 1) the time sequence from transmitter to contact to PPS, 2) the interaction between hardware and software, 3) the time-delay to process the input signals, e.g. T1, T7, and T9, 4) the continuous scanning and memory update, e.g. P2 and P7, and 5) the execution of processing module, e.g. P9. Continuously repeated execution is expressed using the place 'E' and arc 'e'. This modeling was done by using the Colored Petri Net Ver. 3.4.0. [4].

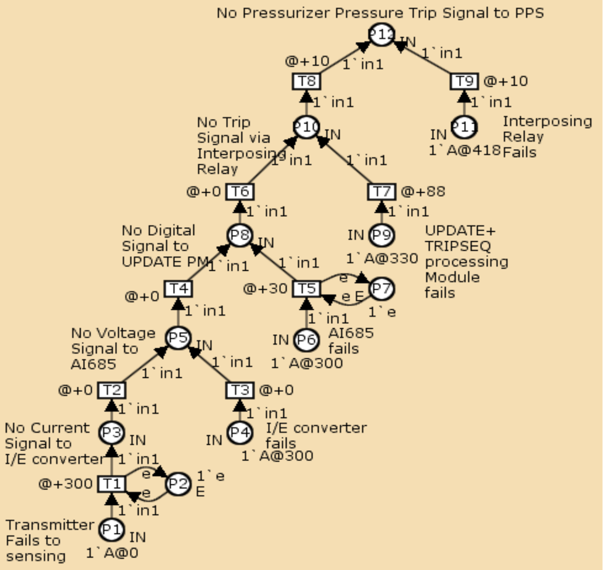


Fig. 3. An Example of Petri Net modeling for Pressurizer Pressure signal.

Fig. 4 is an equivalent Fault Tree model transformed from Fig. 3, using the transformation method introduced in the Section 2.2. The tokens, places and transients in Petri Net correspond to failure data, event and gates in the fault tree, respectively. The fault tree includes, 1) the software fails such as 'AI685 analog input card fails' and 'UPDATE/TRIPSEQ module fails', 2) the sequence of failure from transmitter to contact to PPS, and the interaction between hardware and software. However, it does not express the time-delay to process the input signals, and the continuous scanning and memory update, which are shown in the Petri net model, i.e., Fig. 3. The Fault Tree modeling is useful to get the failure probability and minimal cutset. The failure data are adopted from the PSA Report Shin-kori 3&4 [5] and software failure data is assumed to be 1.5E-6 based on failure of microprocessor. This modeling was done by using the SAREX tool.

The Petri Net and Fault Tree modeling play complementary role in this approach. The information related to time, i.e., time-delay and timing sequence, continuously repeated scanning, memory update, and software execution, is obtained from the Petri net model. The information related to the conventional reliability analysis, i.e., failure probability and minimal cutset, can be obtained from the fault tree model to strengthen the advantages.

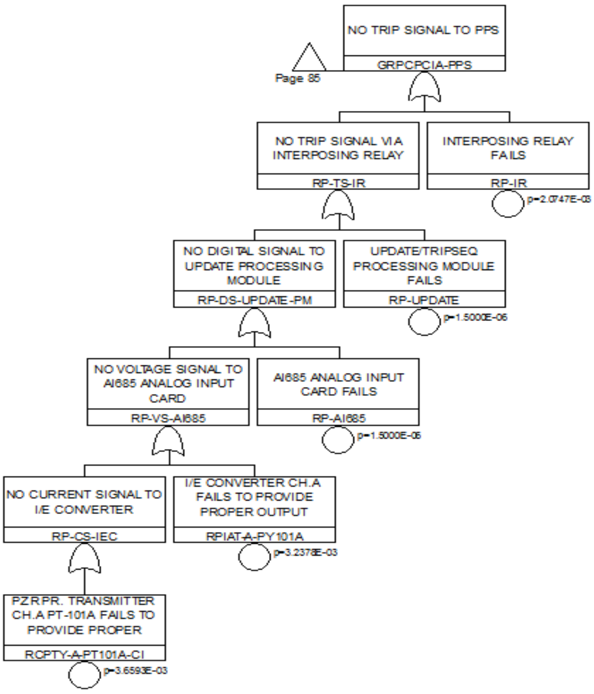

NO TRIP SIGNAL TO PPS
GRPCPCIA-PPS
Page 85
NO TRIP SIGNAL VIA INTERPOSING RELAY
RP-TS-IR
INTERPOSING RELAY FAILS
RP-IR
p=2.0747E-03
NO DIGITAL SIGNAL TO UPDATE PROCESSING MODULE
RP-DS-UPDATE-PM
UPDATE/TRIPSEQ PROCESSING MODULE FAILS
RP-UPDATE
p=1.5000E-06
NO VOLTAGE SIGNAL TO AI685 ANALOG INPUT CARD
RP-VS-AI685
AI685 ANALOG INPUT CARD FAILS
RP-AI685
p=1.5000E-06
NO CURRENT SIGNAL TO I/E CONVERTER
RP-CS-IEC
I/E CONVERTER CH.A FAILS TO PROVIDE PROPER OUTPUT
RPIAT-A-PY101A
p=3.2378E-03
PZRPR. TRANSMITTER CH.A PT-101A FAILS TO PROVIDE PROPER
RCPTY-A-PT101A-CI
p=3.6593E-03

Fig. 4. An Example of Fault Tree modeling for Pressurizer Pressure signal

5. Discussion

This paper proposes a combined method of Petri net and fault tree to analyze the reliability of digital systems. The Petri Net 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. A case study was carried out to demonstrate the feasibility of the combined method.

REFERENCES

[1] T.Aldemir, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NUREG/CR-6942, October 2007.

[2] Lixuan Lu, "An Overview of Digital I&C System Reliability Analysis in Nuclear Power Plants," NPIC&HMI, November 2006.

[3] Andrew Lee, Lixuan Lu, "Petri Net Modeling for Probaiblistic Safety Assessment and its application in the air lock system of a CANDU nuclear power plant," Procedia Engineering 45 (2012) 11 – 20, 2012.

[4] http://cpntools.org/ , Coloured Petri Net, Verson 3.4.0

[5] Final PSA Report for Shin-kori 3&4.