A Development of Common Cause Failure Propagation Paths Identification Method Using Coloured Petri Nets

Ho Bin Yim[*], Jae Min Park, Chang Gyun Lee, Jae Young Huh, Gyu Cheon Lee
KEPCO E&C Co., Inc., 989 Daedeok-daero, Yuseong-gu, Daejeon, 34057
[*]Corresponding author: yimhobin@kepco-enc.com

1. Introduction

The concept of Common-Cause Failure (CCF) first appeared in the aerospace industry several decades ago, and nuclear power industry actively adopted the concept to the nuclear power plant (NPP) system analysis after the TMI accident. Since digital Instrumentation and Control (I&C) systems were applied to the NPP design, the CCF issues once again drew attention from the nuclear power industry in 90’s.

There have been many efforts to resolve the CCF issues worldwide. The U.S. Nuclear Regulatory Commission (NRC) established regulatory guidance addressing the assessment method for the diversity and defense-in-depth concept for nuclear I&C architectures [1, 2]. This method deals with system vulnerabilities caused by CCF. NRC published guidelines on CCF modeling [3], practical usage for Probabilistic Safety Assessment (PSA) [4], and many others. International Atomic Energy Agency (IAEA) also developed a procedure to conduct the CCF analysis for the PSA purpose [5]. All these efforts are mainly for the quantification of the CCF effect on systems, such as parameter estimation. However, IAEA clearly states in its document that many digital systems share resources, including power supplies, communication buses, protective measures. Failures can propagate through these shared resources, potentially leading to CCFs of the digital systems [6]. Thus, the core prerequisite for CCF researches is to identify both CCF-related components and their relationships. Frankly, identification CCF-related components has not been a concern of researcher because CCF can be clearly defined during the Failure Mode and Effect Analysis (FMEA) process by using the Fault Tree Analysis (FTA) or System Block Diagrams (SBD). However, these two major methods have some drawbacks in a practical usage. Modeling FTs of a NPP is a time consuming task, and frequent design changes are not easily and timely updated to the FT models. SBD is very practical way to assume CCF [7]. Nevertheless, the big size of blocks does not reflect the specific details of the NPP and may hide the real threat of CCF. Hence, the SBD method contains high uncertainty in the analysis.

The perspective of CCF propagation paths identification rather belongs to Failure Mode and Effect Analysis (FMEA) philosophy [8] than that of the current CCF issue in nuclear I&C field; the identification of undetectable or hard-to-detect faults acting as root causes in the complex system.

A practical method to identify CCF propagation paths is suggested in this paper. The concept of Coloured Petri Nets (CPN) was applied to plot and map CCF on general diagrams, such as P&ID, logic diagram, or any combination of such diagrams.

2. Methods

The explanation for CCF identification process is given in this section. This method directly uses basic and genuine design documents, such as P&ID, so that the users can reduce analysis time and increase accuracy of the result as well as flexibility of application.

2.1 Coloured Petri Nets

The CPN is a backward compatible extension of the Petri Nets (PN). The CPN preserves useful properties of the PN and at the same time extends initial formalism to allow the distinction between tokens [9]. The CPN has 9 entities of property including those in the PN; places (P), Transitions (T), and arcs (A). Thus, the CPN is a tuple N = ($P, T, A, \Sigma, C, N, E, G, I$) where:
Σ is a set of color sets defined within the CPN model.
C is a color function.
N is a node function.
E is an arc expression function.
G is a guard function.
I is an initialization function.

2.2 CCF Identification Rules

There exist publicly well-known CPN programs, but CCF identification technique in this paper uses only the concept of the CPN. Thus, the fifteen governing rules to use the CPN to identify CCF from general diagrams are defined as below;

1. The place has tokens with Boolean data type and integer type colours, (B, i).
2. The integer type colour is dependent on the Boolean data type colour.
3. When integer i > 0, Boolean B=F (“False”).
4. When i $\leq$ 0, B=T (“True”).

5. Transition is activated when the state of places are satisfied.
6. When the state of place matches “i=0” and input token contains “B=T”, end calculation.
7. i=i-1 when the token goes out to the input port, i+1 when output.
8. The token which contains “B=T” goes out to the output port, always has “i=0”.
9. Initial value for the place designated as the root cause is (F, 1).
10. Block the ark through which the token contains “B=F”.
11. When “the number of open(enable) arks=0”, the place is defined as “a disabled place by CCF”.
12. When “the number of open(enable) arks≥ k” in the “k out of n” logic, the token obtains the value (T,0) for the output.
13. The default token value for input is (T,0).
14. Generate the default input value when no action from the previous transition.
15. Take the maximum “n” among the integer values when “B=F” for the output.

An example of the CPN process to express the AND gate in the logic diagram according to suggested rules is shown in Fig. 1.

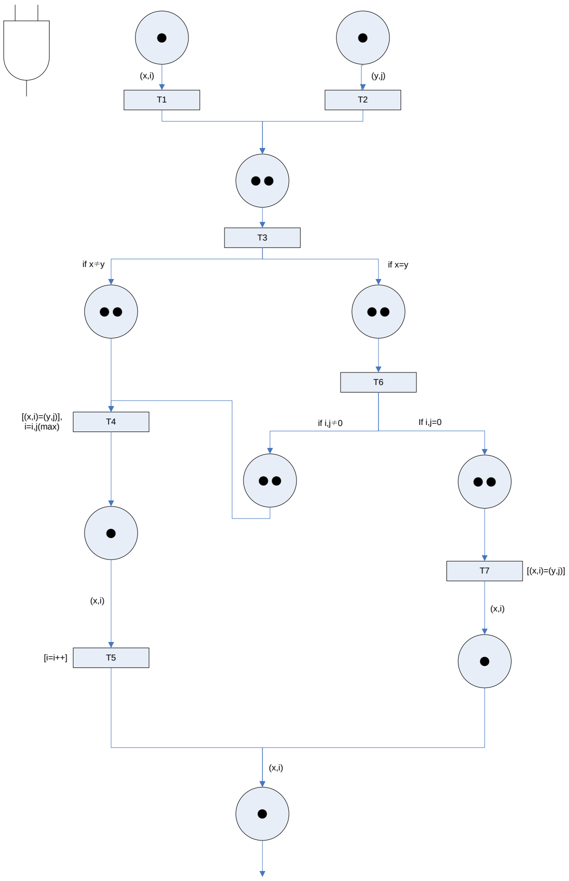

Fig. 1. The internal CPN process for the AND logic gate

2.3 CCF-SIREn

Diagrams such as P&ID are needed to be converted to the certain uniform format to apply suggested rules. *CCF-SIREn* (***C****ommon* ***C****ause* ***F****ailure* ***S****imulated* ***I****nformation* ***R****epresentation* ***En****gine*) is under development for this purpose. *CCF-SIREn* consists of three sub-parts: Map creation, Project creation, and Execution. Important roles for each part are;

Map creation

- Component identification
- Logic gate identification
- Map integrity check

Project creation

- Map scaling
- Map coordinate allocation
- Map combination

Execution

- Project integrity check
- Rule execution

The Fig. 2 shows a brief process of the execution part of *CCF-SIREn*.

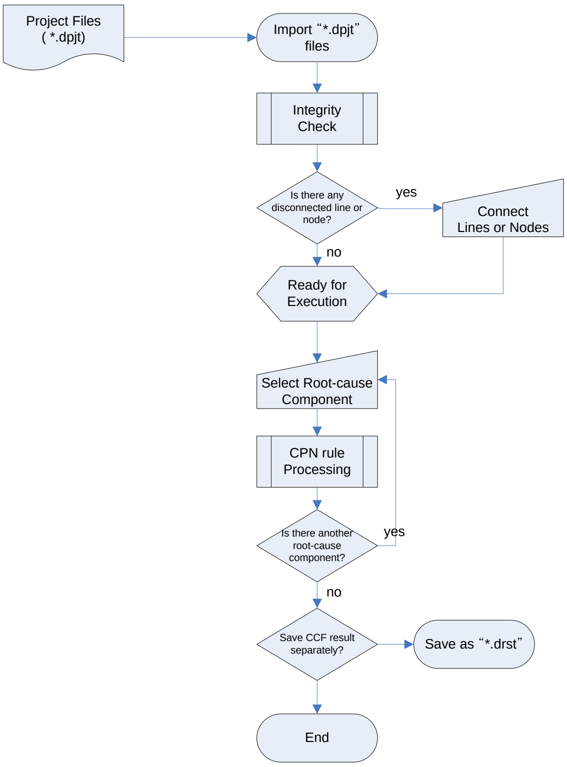

Fig. 2. Execution process of *CCF-SIREn*

CCF-SIREn is targeting to enable four functional modes.

1. Common-Cause Failure Identification Mode
2. Multi-failure Analysis Mode
3. Root-Cause Analysis Mode (Back Propagation)
4. Available Resource Diagnosis Mode

3. Conclusions

Identification of CCF has not been considered as a challenging issue because of its simplicity. However, as the systems become more complex and interconnected, demands are increasing to analyze CCF in more detail, for example, CCF with multiple initiating events or supporting situation awareness of the operation crew. The newly suggested CCF propagation paths identification method, *CCF-SIREn*, is expected to resolve path identification issue more practically and efficiently. *CCF-SIREn* uses general diagrams so that the compatibility and usability can be hugely increased. It also offers up-to-date CCF information with a least analysis effort whenever the ordinary NPP design change processes are made. A back-propagation technique is still under development to find out root-causes from the suspiciously responding signals, alarms and components. The probabilistic approach is also under consideration to prioritize defined CCF.

REFERENCES

[1] U.S. Nuclear Regulatory Commission, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems, Branch Technical Position 7-19, Washington, DC, 2007.

[2] U.S. Nuclear Regulatory Commission, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Instrumentation and Controls, NUREG-0800, Chapter 7, rev.5, Washington, DC, 2007.

[3] U.S. Nuclear Regulatory Commission, Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485, Washington, DC, 1998.

[4] U.S. Nuclear Regulatory Commission, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, NUREG/CR-6268 Rev.1, Washington, DC, 2007.

[5] International Atomic Energy Agency, Procedures for conducting common cause failure analysis in probabilistic safety assessment, IAEA-TECDOC-648, Austria, Vienna, 1992.

[6] International Atomic Energy Agency, Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, No. NP-T-1.5, Austria, Vienna, 2006.

[7] U.S. Nuclear Regulatory Commission, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, Washington, DC, 1994.

[8] U.S. Nuclear Regulatory Commission, Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in Digital Instrumentation and Control Systems, NUREG/IA-0254, Washington, DC, 2011.

[9] J. Kurt, Coloured Petri Nets 2ed., Berlin, Heidelberg, pp.234, 1996.