A frame of reliability model for the safety-critical digital I&C system in NPP

Sung Min Shin[a*]
[a]*Korea Atomic Energy Research Institute, 111, Daedeok-daero 989 Beon-gil, Yuseong-gu, Daejeon, 305-353, Korea*
[*]*Corresponding author: smshin@kaeri.re.kr*

1. Introduction

Currently, most I&C systems in nuclear power plants (NPP) worldwide are being digitalized due to the obsolescence of safety-grade analog components. This shift entails the adoption of new features that do not exist in analog systems. From a safety point of view, the risk caused by the new features should be analyzed in an appropriate framework to ensure the dependability of the entire NPP. However, at present, most of the PSA models for NPP equipped with digital I&C (DI&C) system do not faithfully reflect the features of the newly adopted digital features, and moreover, there is no guidance or consensus on probabilistic safety assessment (PSA) method.

Therefore, in this study, a frame of reliability model for the safety-critical digital I&C system is proposed, in consideration of the representative features of digital system in NPP and the linkage between them.

2. Considerations on a frame of the DI&C reliability model

Although a separate modeling method may be needed to effectively reflect the safety feature of the DI&C system, in this study, a conventional fault tree (FT) format is basically considered for the DI&C system reliability model.

2.1 DI&C system in NPP PSA

From the risk perspective, DI&C related parts in the NPP PSA model can be roughly expressed in figure 1.

A. DI&C induced initial event (spurious operation caused by DI&C system failure)
B. Automatic signal generation failure
C. Manual signal generation failure

In this phase of the study, signal generation failure part will be addressed first. Among safety signal generation failure, the automatic signal generation failure is considered as the priority since the manual signal generation is usually applied as the backup concept of automatic signal generation.

2.2 Typical configuration of DI&C for automatic signal generation

The digital reactor protection system (DRPS) of NPP has some differences in a detailed configuration according to the reactor type and model. To develop a general frame, the DRPS applied to the IDiPS-RPS (Integrated Digital Protection System-Reactor Protection system) developed through the KNICS (Korean Nuclear Instrumentation and control) project, the OPR-1000 (Optimized Power Reactor), and the APR-1400 (Advanced Power Reactor) are investigated, and a typical configuration, as shown in figure 2, is confirmed.

For reference, only the parts related to automatic safety signal generation are shown in this configuration. The notations of each configuration are as follows.

- AIM: Analog input module
- DIM: Digital input module
- PM: Processor module
- CM: Communication module
- F: Fiber optic module (FOM)
- DOM: Digital output module
- AT: Automatic test module
- CPC: Core protection calculator

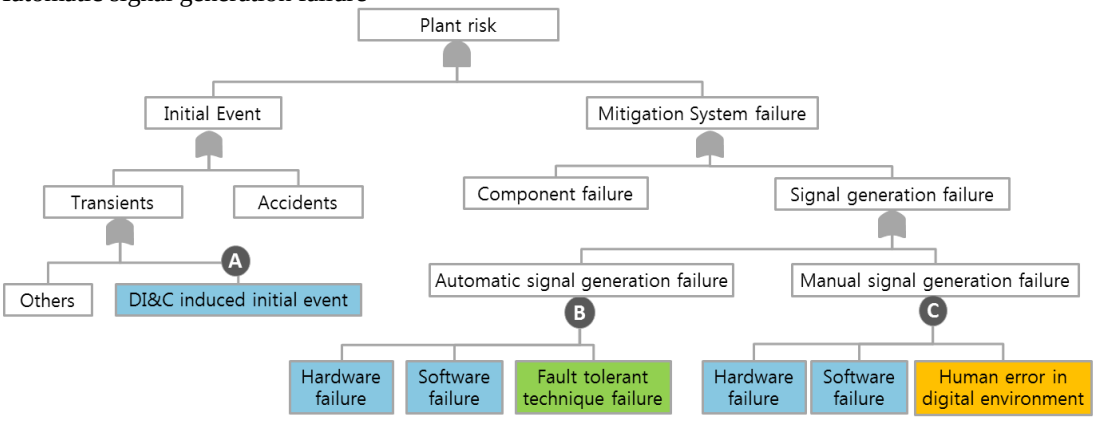

Fig. 1. DI&C related parts in the NPP PSA

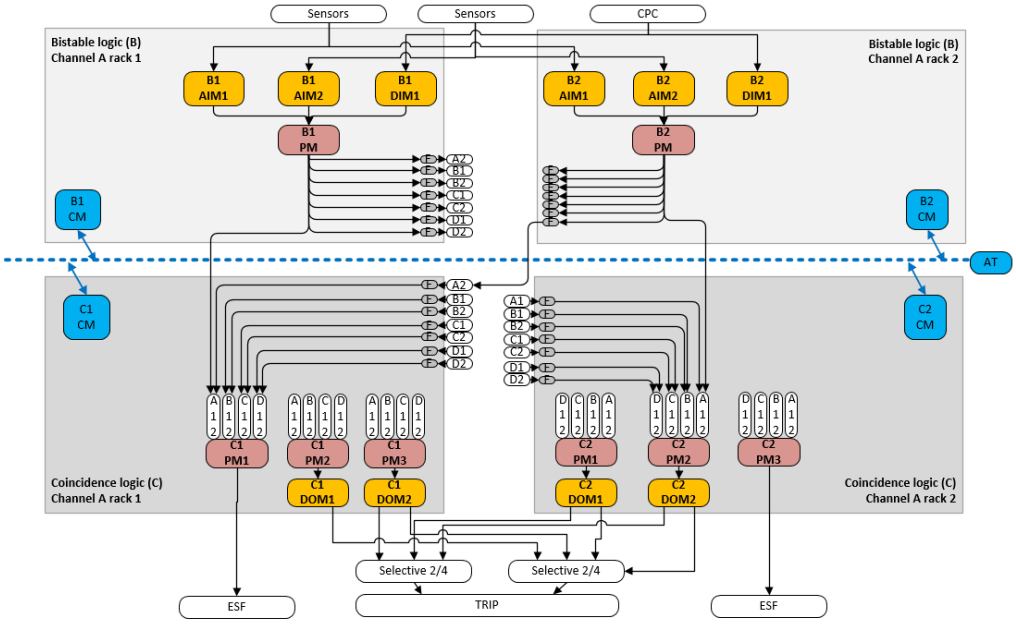

Fig. 2. Typical configuration of DI&C for automatic signal generation

2.3 Requirements for DI&C PSA

The US is also carrying out researches on a reliability evaluation of a DI&C system. In this regard, an interim staff guidance (ISG) is issued to provide the reviewers with detailed requirements to be identified in the DI&C PSA [1]. To identify the requirements to the frame of reliability model for the DI&C system, the review guidelines and additional steps in this reference are checked and marked according to the applicability to this study. The key contents need to be included in the DI&C PSA are selected as follows.

- Specification of scope, boundary condition, and assumption
- System failure mechanism including SW failure
- Identification of common cause failure (CCF) events
- Analysis of network failure
- Verification of credit for defensive design

3. A frame of reliability model for the DI&C system

To implement the requirements identified in chapter 2.3 to the DI&C PSA model, the system is basically divided into standard units, and within each unit, the characteristics of the HW/SW failure and the effects of fault tolerant techniques (FTT) are considered.

3.1 Approaches and assumptions

The top event of the DI&C reliability model is defined as the failure of automatic safety signal generation for each mitigation system in each accident scenario.

To effectively analyze the DI&C system, this study took the module level, such as the input, output, and processor module, as the standard unit. One of the reasons to take this approach is that the different sets of modules are utilized for different safety signal generation.

Within a single module, the categories of failure are largely divided into an HW (hardware) failure, OS (operating system) failure, and AS (application software) failure. It is assumed that the original cause is independent of each other. As for the AS and OS, the two need to be considered separately because the development process, developer, and functions of each is different.

The effect of a fault tolerant technique can be reflected in such a way that the technique detects some portion of each HW, OS, or AS failures in each module and treats them in a fail-safe way so as to not lead to a module failure. The credit of the technique can be considered in this approach together.

3.2 A frame of reliability model

Fig. 3 shows the general frame of the reliability model for a module failure. This frame is applicable to all modules as a basic structure, but depending of the type of module, it may consist of only some of them.

The safety signal is generated by a sequential process in which a value generated in one module is passed to another module and a value generated in that module is passed to the other module. Therefore, the linkage between the modules can be modeled such that the failure of the previous module is input as the 'signal transmission failure' and the failure of that module is connected to another 'signal transmission failure'.

Failures of the HW, OS, and AS in each module leads to a module failure when they are not detected by the FTT or are detected but cannot be handled properly by the FTT. Based on the HW failures illustrated in Fig. 3, if an HW failure is not detected by the FTT, it simply leads to a failure of the module. On the other hand, when an HW failure is detected by the FTT, it can be treated in a fail-safe way when the FTT works properly. Therefore, the reliability of the relevant FTT needs to be considered together in this structure. The reliability of the FTT itself proportionally affects the reliability of the entire DI&C, and the degree of the influence depends on the extent of the fault detection coverage.

In certain cases, various FTTs are applied to a specific module simultaneously, in which case, regarding the detection probability and FTT failure, it is necessary to integrate the effects of the various FTTs or to model the effect of each in detail.

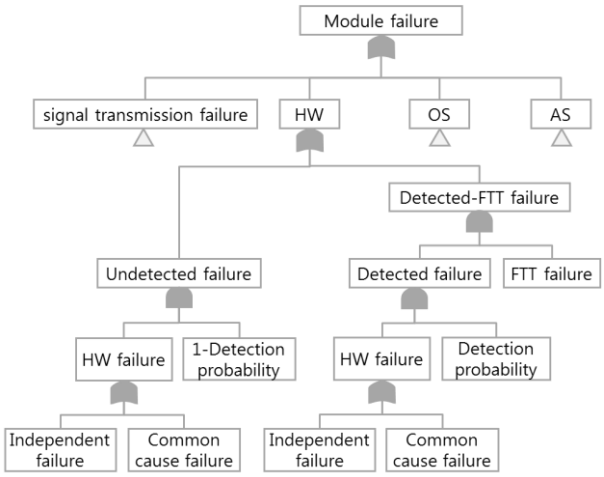

Fig. 3. Frame of reliability model for a module failure

4. Discussions

Although the failure information needs to be obtained to develop the actual reliability model, considering of database could be a constraint on general frame development. Moreover there is no data base providing the necessary information properly yet. Therefore, in the first phase of this study, intentionally, data base was not considered to focus on the development of the general frame of reliability model. On the other hand, the frame of the DI&C PSA developed through this study may suggest some key characteristics of the reliability data to be collected.

There are several factors that need to be confirmed to support the feasibility of the proposed frame: validity of module composition (HW, OS, and AS) and independence between each element, Method to combine the effects (detection probability) and credit of multiple fault tolerant technique, CCF grouping and parameters for SW (OS or AS) failure.

Though each of the topics should be further investigated in future, in this phase, logical validity of the basic structure should be examined first.

5. Concluding remarks

In this study, a method for DI&C PSA modeling for the automatic safety signal generation based on a general reliability model frame of a module. Although there are some assumptions and things to check to confirm the validity of this methodology, author thinks that the complex relationship between elements composing the DI&C system can be objectively modeled by using frames suggested.

ACKNOWLEDGEMENT

This research was supported by Nuclear Research & Development Program of the National Research Foundation of Korea (NRF) grant, funded by the Ministry of Science and ICT (MSIT) (Grant Code: 2017M2A8A4015291).

REFERENCE

[1] U.S. NRC. Review of new reactor digital instrumentation and control probabilistic risk assessment-revision0, DI&C-ISG-03.