Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 27-28, 2016

Single Point Vulnerability Analysis of Automatic Seismic Trip System

Seo Bin Oh [a*], Soon Il Chung [a], Yong Suk Lee [a], Byung Pil Choi [b]
[a]*FNC Technology Co., Ltd.,32 Fl., 13 Heungdeok 1-ro, Giheung-gu, Yongin-si, Gyeonggi-do, Korea*
[b]*Central Research Institute of Korea Hydro & Nuclear Power Co., Ltd. 1312, Yuseong-daero, Yuseong-Gu, Daejeon, 305-343, Korea*
**Corresponding author: ohsb0226@fnctech.com*

1. Introduction

Single Point Vulnerability (SPV) analysis is a process used to identify individual equipment whose failure alone will result in a reactor trip, turbine generator failure, or power reduction of more than 50%[1]. The analysis is useful for minimizing the occurrence of a reactor trip in nuclear power plants (NPPs). By evaluating and determining an SPV, unexpected reactor shutdown can be minimized by improving reliability through intensive maintenance and design modification. Automatic Seismic Trip System (ASTS) is a newly installed system to ensure the safety of plant when earthquake occurs. Since this system directly shuts down the reactor, the failure or malfunction of its system component can cause a reactor trip more frequently than other systems. Therefore, an SPV analysis of ASTS is necessary to maintain its essential performance.

To analyze SPV for ASTS, failure mode and effect analysis (FMEA) and fault tree analysis (FTA) was performed.

2. Automatic Seismic Trip System

ASTS is installed to stop the reactor automatically once massive seismic activity takes place. The purpose of installing ASTS is to prevent human errors through the automatic reactor shutdown process when a large earthquake occurs. In addition, this also elevates the NPP safety posture toward earthquakes and can ultimately improve social acceptability of nuclear power.

Figure 1 shows the reliability block diagram of ASTS. ASTS, although not required for reactor operation, is installed to provide additional protection against a large seismic event. It continuously monitors the acceleration level of seismic sensors and automatically generates a reactor trip signal when the acceleration level exceeds the pre-determined setpoint value. The ASTS is a non-safety system consisting of two channels to initiate reactor trip by using two out of four (2/4) signals. When one sensor module is bypassed during the function test or system maintenance period, the voting logic in the trip logic module is changed from 2/4 to 2/3. Four seismic sensor modules are installed and calculate the seismic accelerations in three orthogonal axes, x, y, and z.

The output circuit breaker of MG-Set (Motor-Generator Set) is selected as the ASTS trip actuation device. The breaker interrupts the power to the Rod Control System to trip the reactor when the ASTS trip logic is initiated.

The ASTS trip status is sent to PMS (Plant Monitoring System) and to PAS (Plant Annunciator System) for alarm.

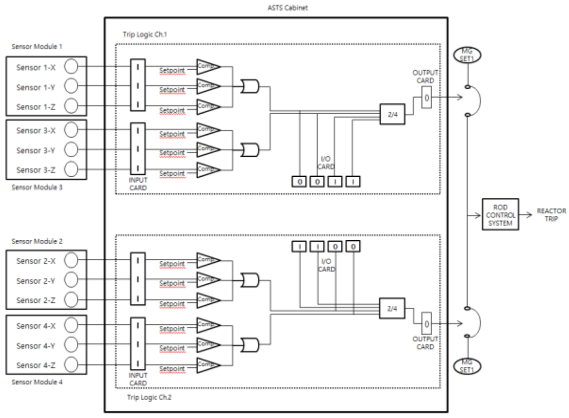

Fig.1. Reliability Block Diagram of ASTS

3. Performance Analysis and Result for Single-Point Vulnerability

3.1 Classification Criteria of the Trip Criticality

SPV equipment is evaluated by utilizing the trip criticality classification criteria. Trip criticality classification criteria is classified in four class ; TC-1, TC-2, TC-3, Non Criticality(NC). Classification Criteria of the trip criticality is shown in Table I[1].

Table I: Trip Criticality Classification Table

Trip Criticality	Classification Criteria
TC-1	○ The effect of the loss of a single device function is as follows: reactor/power generation is stopped, more than 50% of the power reduction
TC-2	○ The effect of the loss of a single device function is as follows: less than 50% of the power reduction ○ The effect of the loss of two devices function is as follows: reactor/power generation is stopped, more than 50% of the power reduction
TC-3	○ The effect of the loss of two devices functions is as follows: less than 50% of the power reduction ○ The effect of the loss of three or more devices functions is as follows: reactor/power generation is stopped, more than 50% of the power reduction
NC	Failure does not induce the development of reactor trip/power reduction in the function of the target device.

3.2 Failure Mode and Effect Analysis (FMEA)

FMEA is a systematic process to identify the failure mode of the target system components and evaluate the results. The purpose of FMEA performed in this study is to identify possible failure modes for each individual component of target system and evaluate the possibility of reactor trip occurrence and shutdown.

Components effecting on the reactor trip deduced from the FMEA of ASTS performed in this study are as follows:

- Digital Output (D/O) Card, Digital Input (D/I) Card, Analog Input (A/I) Card
- Seismic Sensor Modules
- MG Set Trip Relay

FMEA example of ASTS performed in this study is shown in Table II. D/O card, D/I card, A/I card, seismic sensor and trip relay is generated by the malfunction. Because the 2/4 coincidence logic is applied for the reactor trip, the reactor trip does not occur in the single failure. Therefore, equipment is evaluated as the TC-2. It does not affect the power reduction. In addition, loss of power does not affect reactor trip. It loses function only.

Table II: FMEA Example of ASTS

List	Name	Failure Mode	Function	Trip Criticality
1	ASTS Cabinet CH.1 Digital Output TB4-1	Spurious Actuation (Operation)	○ Detection of seismic wave by sensor module ○ Reactor trip by the trip signal of digital output module MG-Set	TC-2
2	ASTS Cabinet CH.1 Digital Input TB/DI-1 (L37)	Spurious Actuation (Operation)	○ Detection of seismic wave by sensor module ○ Reactor trip by the trip signal of digital input module MG-Set	TC-2
3	ASTS Cabinet CH.1 Analog Input TB/AI-1 (L1)	Spurious Actuation (Operation)	○ Detection of seismic wave by sensor module ○ Reactor trip by the trip signal of analog input module MG-Set	TC-2
4	PLC CH.1 MG-Set Trip TB4-1 (Field Termination)	Spurious Actuation (Operation)	○ Reactor trip caused by free fall of control rod which starts with stop signal from channel 1, 2 which are transferred to MG-Set 1, 2 respectively so that cut the power for the MG-Set	TC-2
5	PLC CH.2 MG-Set Trip TB4-2 (Field Termination)	Spurious Actuation (Operation)	○ Reactor trip caused by free fall of control rod which starts with stop signal from channel 1, 2 which are transferred to MG-Set 1, 2 respectively so that cut the power for the MG-Set	TC-2
6	Seismic Sensor Modules 1 (Accelerometer)	Spurious Actuation (Operation)	○ To apply the two out of four(2/4) logic for reactor trip. ○ Reactor trip activated if the one or more of three axis (x, y, z) of seismic acceleration.	TC-2
7	Seismic Sensor Modules 3 (Accelerometer)	Spurious Actuation (Operation)	○ To apply the two out of four(2/4) logic for reactor trip. ○ Reactor trip activated if the one or more of three axis (x, y, z) of seismic acceleration.	TC-2

3.3 Fault Tree Analysis (FTA)

FTA is a logical analysis method to deduce all possible failure modes which can cause the unavailability of system, considering all system operating conditions, and describes the state of system which loses its function. Based on the SPVs found with FMEA, FT modeling was performed.

The considerations for developing the FTA of ASTS are as follows:

- Equipment failure and failure of equipment operation by the malfunction or wrong signal
- NC equipment which does not affect reactor trip is not included in modeling

Sensor detecting an earthquake wave supplies the signal to output card through the input card. When the stop signal received from the output card is generated to the two channels, they are delivered to MG-Set 1, 2 respectively. The power of the Rod Control System is blocked. Therefore, reactor trip is made by the falling of reactor control rods.

Figure 2 shows the FT modeling of ASTS.

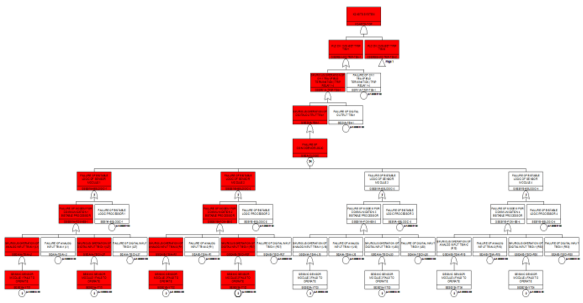

Fig.2. Fault Tree Modeling of ASTS

4. Conclusions

In this study, FMEA and FTA methods were performed to select SPV equipment of ASTS. D/O, D/I, A/I card, seismic sensor, and trip relay had an effect on the reactor trip but their single failure will not cause reactor trip. In conclusion, ASTS is excluded as SPV.

These results can be utilized as the basis data for ways to enhance facility reliability such as design modification and improvement of preventive maintenance procedure.

REFERENCES

[1] KHNP, Final Report Shin-Kori Unit 1,2,3,4 Construction of the Array Model and FMEA/FTA Shin-Wolseong Unit 1,2 System, 2014.
[2] EPRI TR-1008121, Generation Risk Assessment (GRA) Implementation Guide, G. Sliter, 2004.
[3] Jin Kwon Jeong, etc., The Design of Automatic Seismic Trip System for the Nuclear Power Plants, KNS, 2010.