Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 29-30, 2015

Review of Byzantine General Problems in the Reactor Protection System of Korean Nuclear Power Plants

Eungse Oh and Yungoo Kim

Korea Hydro and Nuclear Power Co., Ltd, Central Research Institute, Daejeon, Korea
E-mail: eungse.oh@khnp.co.kr, ygkim.stpn@khnp.co.kr

1. Introduction

For consented logical decisions in the complex multiple computing systems, a "majority voting" is one of the method that has a long history form the analog computing era. For some error or fault cases, a computer system may provide contradictory information to other computer systems that interfaced with. This kind of complex error scenario is known as a Byzantine General Problem and the error is called a Byzantine Error (BE). [1]

The BE is now considered as one of the plausible common-cause failure in the nuclear power plant's (NPP) computer systems. [2]

The Reactor Protection System (RPS) in the Korean NPP consists of multiple redundant digital computer systems to increase system availability and redundancy.

This system architecture is inherited form the well proved analog system's architecture.

Failure modes and effects on the RPS system functions are reviewed when a BE assumed in the system's decision making logic path.

2. General Decision-making Logic in the RPS

Generally, the RPS in the Korean NPP consists of four redundant channels. Each channel has dedicated input sensors (e.g., temperature, pressure), a comparison logic part (aka, Bistable Logic), and a majority voting logic part (aka, Local Coincidence Logic) to generate a initiation signal for reactor trip. The trip signal generation process can be summarized as follows:

a. A comparison logic part receives a plant variable value from a dedicate sensor.
b. The comparison logic part compares the variable value with a pre-determined value (setpoint).
c. If the variable value exceeds the setpoint, the comparison logic part generates a reactor trip signal for voting (RT_{vote}).
d. The comparison logic part sends the RT_{vote} to the own voting logic part and other channels' voting logic part.
e. A voting logic part in a channel receives the RT_{vote} of own channel and other RT_{vote} from the other channels.
f. If voting logic part receives more than two RT_{vote}s, the part generates final reactor trip initiation signal (RT_{init}) for the own channel.

Both RT_{vote} and RT_{init} are binary signal (i.e., TRUE or FALSE).

During the process of d. and e., a comparison logic part may deliver contradict RT_{vote} signals to the downstream voting logic parts (own and other channels), which is denoted a traitor [1].

3. Assumptions for BE Review

For the clear and conservative BE reviews, following assumptions are applied.

a. One RPS channel is bypassed for maintenance.

Bases: With one channel bypassed, the RPS shall perform a reactor trip function [3]. The voting logic part only considers three inputs (2-out-of-3 logic) generated from comparison logic part for the decision-making.

b. A traitor talks more false information than true information to the linked parts.

Bases: If false information is less than true information, the BE can be considered as one of the single failure [3].

If one computer has a BE in a computer system that consists of three decision-making computer, no decision can be made by the system is well known [1]. In this case, the computer system uses only two inputs for decision-making.

4. One Channel BE Review

For this review, we assume that Channel A acts as a traitor, but Channel B and C acts as a royal general [1]. At this time, Channel D is assumed in bypassed status.

The Channel A's comparison logic part acts as traitor and sends false signals to any of Channel (A, B, C) voting logic part. Let define a true signal as "1" and a false signal as "0".

For example, assume Channel A sends RT_{vote} signals (1, 0, 0) to Channel (A, B, C) voting logic part respectively.

The voting logic part of each channel receives (1, 1, 1); (0, 1, 1);(0, 1, 1) respectively.

Thus, majority voting result of each channel becomes Channel A = Trip; Channel B = Trip; Channel C = Trip.

The result shows that one channel BE does not affect the RPS's trip function.

Detailed truth table of one channel BE case is shown at Table 1. The colored boxes in the "Trip(*X*)" column of the table shows the RPS channel is in the trip initiation status.

Table 1. One RPS Channel BE Truth Table

Vote(A)			Vote(B)			Vote(C)			Trip(A)			Trip(B)			Trip(C)		
A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
0	0	0	1	1	1	1	1	1	0	1	1	0	1	1	0	1	1
0	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1
0	1	0	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1
1	0	0	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1

Note: 0 = false, 1 = true, A, B, C = Channel

5. Two Channels BE Review

Let assume Channel A and B are traitor and Channel C is royal. In this case, the RPS may or may not act as normal trip function depend on the BE mode.

The truth table of these failure cases is shown at Table 2.

These common-cause BE results can be bounded at a more conservative RPS failure case that no channel can generate a trip signal. In this rare failure mode, a diverse protection system, which is designed to immune to the common-caused failure mechanism, acts to trip the reactor.

Table 2. Two RPS Channels BE Truth Table

Vote(A)			Vote(B)			Vote(C)			Trip(A)			Trip(B)			Trip(C)		
A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
0	0	0	0	0	0	1	1	1	0	0	1	0	0	1	0	0	1
			0	0	1	1	1	1	0	0	1	0	0	1	0	1	1
			0	1	0	1	1	1	0	0	1	0	1	1	0	0	1
			1	0	0	1	1	1	0	1	1	0	0	1	0	0	1
0	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	0	1
			0	0	1	1	1	1	0	0	1	0	0	1	1	1	1
			0	1	0	1	1	1	0	0	1	0	1	1	1	0	1
			1	0	0	1	1	1	0	1	1	0	0	1	1	0	1
0	1	0	0	0	0	1	1	1	0	0	1	1	0	1	0	0	1
			0	0	1	1	1	1	0	0	1	1	0	1	0	1	1
			0	1	0	1	1	1	0	0	1	1	1	1	0	0	1
			1	0	0	1	1	1	0	1	1	1	0	1	0	0	1
1	0	0	0	0	0	1	1	1	1	0	1	0	0	1	0	0	1
			0	0	1	1	1	1	1	0	1	0	0	1	0	1	1
			0	1	0	1	1	1	1	0	1	0	1	1	0	0	1
			1	0	0	1	1	1	1	1	1	0	0	1	0	0	1

6. Conclusions

For this review, one channel and two channels of BE problems in the RPS trip function are considered. If a BE occurs in any one channel of the RPS, the systems trip function has no harm affects from the BE. If two BEs occur in any channels of the RPS, the systems trip function may or may not work properly.

This BE review method can be applied to other decision-making parts of the protection system in NPP.

REFERENCES

[1] Leslie Lamport et. al., "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982.

[2] RIL-1002, "Identification and Analysis of Failure Modes in Digital Instrumentation and Control (DI&C) Safety Systems - Expert Clinic Findings, Part 2," U.S. NRC, September 2014.

[3] IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," December 1991