Safety Improvement for RPS of AGN-201K Research Reactor with PLCs and FPGAs

Jiye Jeong , Gyunyoung Heo*
Department of Nuclear Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea
**Corresponding author: gheo@khu.ac.kr*

1. Introduction

Transition from conventional analog technology to advanced digital technology is a global trend and the use of digital technology is instrumentation and control (I&C) systems of nuclear power plants and research reactors has increased since last decade [1]. The I&C systems with various digital platforms have been studied. For safety systems, Programmable Logic Controller (PLC) and Field Programmable Gate Array (FPGA) have been considered. In case of PLC, the nuclear power plants in Korea have selected the platform for safety systems, but because of the vulnerability to cyber-attack and other related issues of microprocessor-based software systems, the digital model with FPGA has been researched as an alternative in the future [2][3].

No matter what kind of architectures are introduced, the digital model with single platform is still weak in common cause failure (CCF) seriously even though the digital system has several channels redundantly.

To propose a potential solution for the significant problem of CCFs, the concept of digital hybrid model which means that two platforms with PLC and FPGA has been investigated in this study. The case example was applied to an educational research reactor, AGN-201K at Kyung Hee University. Authors have two goals: The AGN-201K has the reactor protection system (RPS) with three safety channels composed of several analog equipment. It has also another digital console, but this is for only monitoring purpose. Along with the technical trend, AGN-201K may require the upgrade of obsolescent analog RPS in the future, so this study attempted to delineate the method to cope with the digital RPSs, which is the first goal. The other is it is easier to see how much design change can affect unavailability due to its simple structure.

The new digital hybrid model of RPS of the AGN-201K is designed to have four safety channels. In order to make a balance between platforms, the number of safety channels of RPS of AGN-201K was adjusted to even number. The combination of such four channels can be assigned upon the design requirements; for example, four channels of PLCs or FPGAs, or two channels of PLCs and FPGAs respectively.

The aim of this research is to compare the digital hybrid model with the current system and single platform system on unavailability by fault trees analysis (FTA) developed using AIMS-PSA software.

2. Methods and Results

In this section, risk-informed safety improvement procedure and the results of the analysis performed on the safety improvement approaches are presented step-by-step along with the conventional one, four channels of PLCs and FPGAs, and two channels of PLCs and FPGAs respectively.

2.1 System Modeling of RPS

From the configuration of RPS of AGN-201K (Fig. 1), top-level of fault tree model was developed from the identification of the system failure criteria via analysis of scram logic [4].

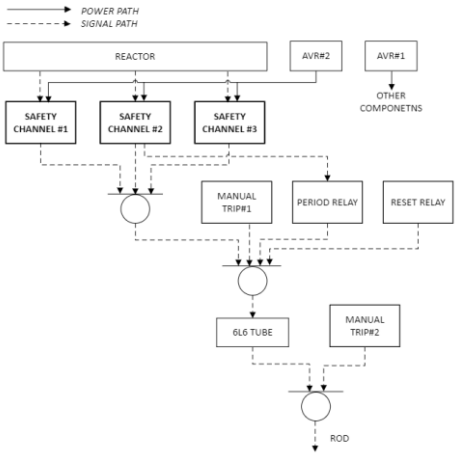

Fig. 1. Configuration of RPS of AGN-201K

The three safety channels of current RPS consists of several analog components; neutron instruments, rate meters, log meters, relays, power supplies, rectifiers, and single rod accessories [3]. The four dominant contributors' cutsets of analog model are shown in Table 1. In this model, the important basic event is failure of s-relay of all channels.

Table 1: Cutset probabilities of 3 channels of analog RPS

No	Cutset Probability	FV (Fussell-Vesely)	Event Description
1	7.805E-08	99.9979	S-RELAY#1,2,3
2	7.522E-13	00.0010	S-RELAY#2 AND S-RELAY#1,3
3	4.531E-13	00.0006	AVR#1 AND S-RELAY#2,3
4	4.531E-13	00.0006	S-RELAY#1,3 AND AVR#1

The three safety channels of analog RPS are changed to four safety channels of digital platforms as described in Section 1. In other words, safety channel #2 was re-designed to safety channel #2-1 and safety channel #2-2 for redundancy as shown in Fig. 2. In the four channels model, the channel trip signal is 1 out of 4 scheme so the number of channel trip signal is same to the current model of RPS.

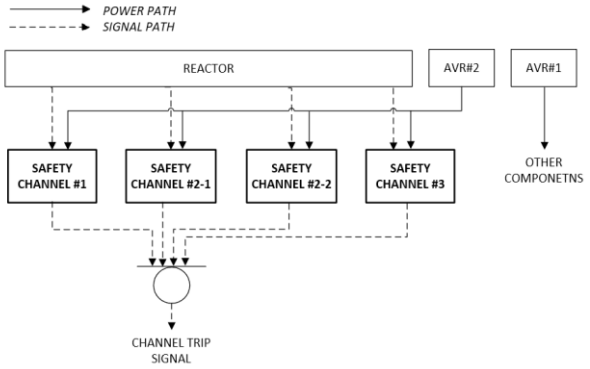

Fig. 2. Configuration of four channels model of digital

2.2 Four Channels of PLCs

This section explains how the four channels can be composed of PLCs and the unavailability is evaluated. The PLCs which are embedded-systems can accurately control relatively simple functions, while the configuration of their platform is complex.

Fig. 3 shows the top-level fault tree model of four channels with PLCs, which is considered the failure rate of eight modules of PLC; base board, power supply module, processor module, communication module, digital input module, digital output module, analog input module, and analog output module [5].

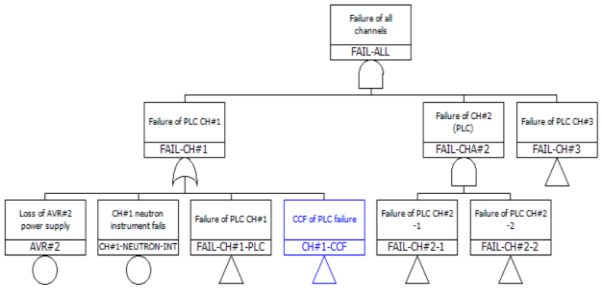

Fig. 3. Top-level model of fault tree for four channels of PLCs

In addition, the alpha factor was selected for the generic rate CCF of PLCs [6]. In this calculation, the four dominant contributors' cutsets of this model are presented in Table 2. In this model, the critical basic events are the CCF of four channels or three channels.

Table 2: Cutset probabilities of 4 channels of PLC

No	Cutset Probability	FV	Event Description
1	4.190E-7	65.17	CCF (4/4)
2	2.239E-7	34.82	CCF (3/4) of CH#1,2-1,2-2
3	4.377E-12	0.0007	Processor failure of CH#1 AND CCF (3/4) of CH#2-1,2-2,3
4	4.377E-12	0.0007	Processor failure of CH#2-1 AND CCF (3/4) of CH#1,2-2,3

2.3 Four Channels of FPGAs

The top-level model of fault tree for four channels of FPGAs is same to Fig. 3 except of the platform used.

The FPGAs are the platform used for integrated systems, so they can perform complex functions faster. There are several distinct aspects from those of PLCs.

The failure rate of five modules of FPGA was considered; processor board, analog input board, analog output board, digital input board, digital output board [7]. Also, the same alpha factor of the digital model for PLCs is selected for the CCF modelling of FPGA [6]. The four dominant contributors' cutsets of this model are presented in Table 3. The FPGA model is safer than the PLC model, however, the CCF of four channels or three channels are still highly risky.

Table 3: Cutset probabilities of four channels of FPGA

No	Cutset Probability	FV	Event Description
1	7.740E-08	65.17	CCF (4/4)
2	4.136E-08	34.83	CCF (3/4) of CH#1,2-1,2-2
3	2.550E-13	0.0002	Digital input board of CH#1 AND CCF (3/4) of CH#2-1,2-2,3
4	2.550E-13	0.0002	Digital input board of CH#2-1 AND CCF (3/4) of CH#1,2-2,3

2.4 Digital Hybrid of FPGAs and PLCs

We found the CCF of all or three channels of RPS would be the top-ranking contributor, which is also unavoidable in the single platform architecture. Therefore, the independent separation of the platform may be able to reduce this result. The digital hybrid architecture of PLCs and FPGAs was modeled and its unavailability was evaluated.

The digital hybrid model consists of two channels of FPGAs (CH#1, CH#2-1) and two channels of PLCs (CH#2-2, CH#3) as shown in Fig. 5.

The same methodology described in the Section 2.2 and 2.3 is used to calculate the generic rate CCF for digital hybrid model [6].

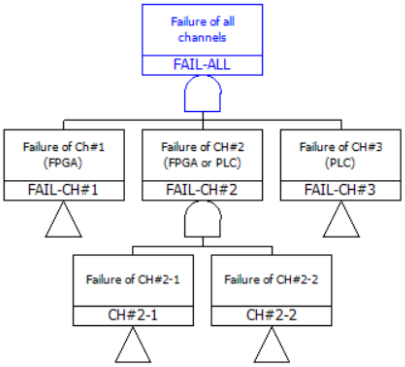

Fig. 4. Top-level model of fault tree for digital hybrid model

The four dominant contributors' cutsets of this model are presented in Table 4. The CCF of FPGA and PLC is important basic event in digital hybrid model but the availability is significant improved comparing with the PLC model and FPGA model.

Table 4: Cutset probability of digital hybrid RPS

No	Cutset Probability	FV	Event Description
1	1.008E-12	99.67	CCF of FPGA AND CCF of PLC
2	1.649E-16	0.016	Processor failure of PLC CH#3 AND CH#2-2 AND CCF of FPGA
3	1.300E-16	0.013	Analog output failure of PLC CH#3 AND Processor failure of PLC CH#2-2 AND CCF of FPGA
4	1.300E-16	0.013	Processor failure of PLC CH#3 AND Analog output failure of PLC CH #2-2 AND CCF of FPGA

Based on the results of this study, the analog model (Model No.1) is more available than two digital models which are four channels of PLC (Model No.2) and FPGA (Model No.3). In addition to this, the CCF is highly significant basic event for all models. However, by using two different platforms (PLCs and FPGAs) in one model (Model No. 4), the unavailability of the RPS could be improved dramatically as shown in Table 5.

Table 5: Unavailability of each model

No	Model	Unavailability
1	Baseline (Three channels of Analog)	7.850E-08
2	Four channels of PLCs	6.429E-07
3	Four channels of FPGAs	1.188E-07
4	Digital hybrid (Two channels of PLCs + Two channels of FPGAs)	1.012E-12

3. Conclusions

Since the digital model is much easier to maintain and control systems, the trend of power industries has been getting digitalized. It was obvious that two independent platforms can achieve higher availability due to the reduction of CCFs so this paper focused on how much the digital hybrid models are better than the single platform models.

However, using two different platforms means that two independent software were required and the cost would be increased. In this reason, the cost benefit analysis of the digital hybrid model is needed to be conducted as a next step.

ACKNOWLEDEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP: Ministry of Science, ICT and Future Planning) (No. 2017M2B2B1072806)

REFERENCES

[1] Rahman KU, Heo G, Kim M, Muhammad Z. Formulation and Reliability Feature Analysis of Analog, Digital & Hybrid I&C Architectures for Research Reactors. International Conference On Nuclear Engineering(ICONE) - Prague (Czech Republic) 2014.07.
[2] Rahman KU, Jin K, Heo G. Risk-informed design of hybrid I&C architectures for research reactors. IEEE Trans Nucl Sci 2016;63:351–8.
[3] Ibrahim A, Jung J, Heo G. Design Verification Enhancement of FPGA-based Plant Protection System Trip Logics for Nuclear Power Plant. KNS – Jeju 2016.05
[4] Ibrahim A, Heo G. Safety Improvement for AGN-201K Research Reactor Shutdown System. International HANARO Symposium – Deajeon (Korea) 2019.04
[5] Korea Atomic Energy Research Institute (KAERI). Reliability Analysis of PLC Safety Equipment, KAERI/CM-933/2005
[6] U.S. Nuclear Regulatory Commission. CCF Parameter Estimations, 2015 Update 2016.
[7] Lee JK, Jeong KI, Park GO, Sohn KY. A Quantitative Reliability Analysis of FPGA-based Controller for Applying to Nuclear Instrumentation and Control System. Korea Institute of Electronic Communication Science (KIECS), Vol.9 No.10, 2014
[8] Korea Atomic Energy Research Institute (KAERI). The Common Cause Failure Probability Analysis on the Hardware of the Digital Protection system in Korean Standard Nuclear Power Plant, KAERI/TR-2908/2005