Development of Safety Grade Control Platforms for Safety I&C System Against Common Cause Failure

Jong Gyun Choi, Chang Hoi Kim
Korea Atomic Energy Research Institute, 989-111, Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Korea
**Corresponding author: choijg@kaeri.re.kr*

1. Introduction

The I&C system in nuclear power plants consists of multiple systems such as reactor regulating system, reactor protection system, engineered safety features actuation system and monitoring & indicator system to provide independent echelons of defense. However, common cause failure (CCF) can disable one or more echelons of defense although each system employed the multiple redundancies.

Two diverse control platforms have been developed for application to safety I&C systems which have capability to mitigate CCFs under the project funded by the Korean Ministry of Trade, Industry & Energy. In this project Susan E&S develops the microprocessor based control platform named SPLC and Doosan Heavy Industry is in charge of developing the FPGA based control platform named DFLC-N.

This paper describes the typical diversity strategies which can be implemented in safety I&C systems and introduces two safety grade control platforms being developed to improve the diversity of safety I&C systems.

2. Development of Safety I&C system against CCF

2.1 Diversity strategies in safety I&C system

The typical safety system architecture against CCF is shown in Figure 1 [1, 2]. The first diagram shows the coequal diverse safety system in which two separate subsystem X and Y process data to generate safety actuation signals independently. The input data are provided through separate paths and the safety actuation signals from each subsystem are transmitted across separate paths to actuation devices. Subsystems X and Y are developed according to the safety class and both can provide full coverage against all design basis events. The second diagram shows the primary and secondary diverse safety system which is similar to the coequal diverse safety system in that it has two separate subsystems. However, subsystem X is treated as the primary system and subsystem Y is the secondary system in this architecture. The distinction between the primary and secondary subsystems can be seen in terms of the coverage of PIEs and/or the safety classification. The third architecture can be used only when operator has sufficient time and information to generate safety action signals in case of the failure of subsystem X.

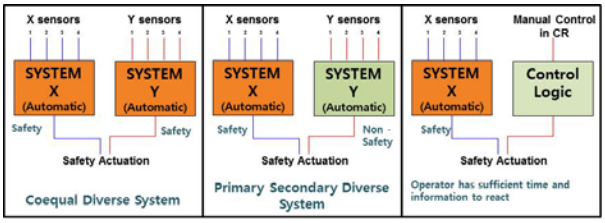

Fig. 1. The typical diverse architecture

As shown in Figure 2, the design diversity between subsystem X and subsystem Y can be technically implemented with one of three strategies as follows (listed in decreasing order of effectiveness) [2]:

- **I.** Fundamentally Different Technologies (Analog vs. Digital)
- **II.** Distinctly Different Technologies (Microprocessor vs. FPGA)
- **III.** Digital Technology Variation (Intel vs. Motorola)

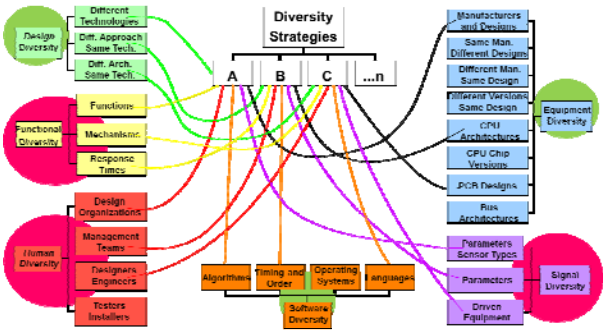

Fig. 2. Diversity Attributes

The strategy I has the most comprehensive impact on system diversity because this strategy provides inherently the other associated diversities such as equipment diversity and software diversity between subsystem X and Y. However, it is not easy to adopt this strategy in reality since the most industry has changed from analog to digital and manufactures do not

provide nuclear I&C system based on analog technology any more.

The strategy II inherently provides the system with some measures of equipment diversity and software diversity and the strategy III inherently contributes some limited degree of equipment diversity and logic diversity.

2.2 Development of Safety Control Platforms

One of the objects of R&D project funded by the Korean Ministry of Trade, Industry & Energy is to develop two safety grade control platforms having diversity each other for application to coequal diverse safety system according to the diversity strategy II. Two different manufactures, Doosan Heavy Industry and Susan E&C, are involved in this project. Susan E&S develops the microprocessor based control platform named SPLC and Doosan Heavy Industry is in charge of developing the FPGA based control platform named DFLC-N.

If these two platforms are applied to subsystem X and Y respectively in coequal system or primary and secondary system, the system can have diversity attributes as described in Table 1.

Table 1: Diversity Measure between Two Platforms

Diversity Attributes	**Applied Approach**	**Details**
Design	Different Approach within a technology	CPU vs. FPGA
Function	N/A(Plant Dependent)	
Life Cycle	Different company	Susan vs. Doosan
Equipment Manufacturer	Different manufacturers of fundamentally different designs	Susan vs. Doosan
Logic Processing Equipment	Different logic processing Architecture	Serial vs. Parallel
Logic	Different algorithms, logic, and logic architecture	C vs. VHDL
Signal	N/A(Plant Dependent)	

2.3 SPLC Design

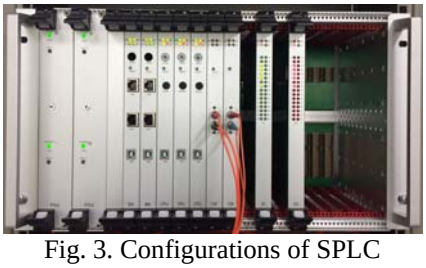

Fig. 3. Configurations of SPLC

The SPLC consists of various modules such as a power module, a processor module, communication module, digital input/output modules, analog input/ output modules. The SPLC installs two independent power modules in a rack as shown in Figure 3. The power module has a 100% power supply capability for each. Accordingly, even when there is a fault in one power module, it does not affect the SPLC operation. SPLC is also designed with full triple modular redundant architecture from input terminal to output terminal. This architecture allows the system to operate continually in the presence of any single point of failure within the platform. The general hardware specification of SPLC is described in Table 2.

Table 2: SPLC Specification

Configuration	Item	Specification	Description
Processor Module	Microprocessor	MCF54453	32bit
	Clock	266MHz	
Analog I/O Module	Range	0V~10V, 4mA~20mA	16 CH (Current/Voltage)
	Accuracy	±0.1%	16bit AD/16bit DA
	Update Time		
Digital I/O Module	Range	0V ~ 24V, 48V	32CH
	Update Time	5ms	
Network Comm. Module	Speed	20Mbps/64node	1CH (TX/RX separated)
	Protocol	TDMA	STAR

2.3 DFLC Design

Fig. 4. Configuration of DFLC-N

DFLC-N is a safety control platform based on FPGA as shown in Figure 4. It includes a general purpose processor module, a complex processor module, communication module, digital input/output modules, analog input/output modules. The complex processor module is a sort of one board controller which contains digital I/O channels, analog I/O channels and data-link communication ports in it. DFLC-N is designed with four independent serial bus architecture which enables four processor modules to operate independently in a rack. The general specification of DLFC-N is described in Table 3.

Table 3: DFLC-N Specification

Configuration	Item	Specification	Description
Processor Module	FPGA	Microsemi	Min. 10ms scan-time
	Clock	80 MHz	
Analog I/O Module	Range	0V~10V, 4mA~20mA	8CH (Current/Voltage)
	Accuracy	±0.1%	18bit AD/16bit DA
	Update Time	5ms	
Digital I/O Module	Range	0V ~ 24V	32CH
	Update Time	5ms	

Datalink Comm. Module	Speed	5Mbps	4CH (TX/RX separated)
	Protocol	Based on UART-232	
Network Comm. Module	Speed	20Mbps/64node	1CH (TX/RX separated)
	Protocol	TDMA	STAR

3. Conclusions

Two control platforms have been developed for application to safety I&C systems under the project funded by the Korean Ministry of Trade, Industry & Energy. In this project Susan E&S develops the microprocessor based control platform and Doosan Heavy Industry is in charge of developing the FPGA based control platform

In this paper the typical diversity strategies implemented in safety I&C systems were described and the design concept of two safety grade platforms was introduced for mitigating the CCF vulnerabilities.

These platforms have been developed under a quality assurance and a configuration management program with a strict V&V process for safety application.

REFERENCES

[1] IEC 61513: Nuclear power plants – Instrumentation and control important to safety – general requirements for system, 2011

[2] NUREG/CR-7007: Diversity Strategies for Nuclear Power Plant Instrumentation and Control System, 2010.