Conceptual Design of Nuclear Integrated Safety System

Kwang Seop,Son *, Dong Hoon, Kim

Korea Atomic Energy Research Institute (KAERI)
P. O. Box 105 Yuseongu, Daejeon, 305-600, Republic of Korea
ksson78@kaeri.re.kr

1. Introduction

The Safety system in nuclear power plant actuates control rods to trip a reactor or en engineered safety feature-component control system, if process variable exceed a set point that limits plant operation. In existing safety system, 4 channels are configured and in one channel, physically isolated dual or triple system is configured. Also Interfaces among Reactor Core Protection System (RCOPS), Reactor Protection System (RPS), Engineered Safety Feature-Component Control System (ESF-CCS), Qualified Indication & Alarm System-P (QIAS-P), are separated. In this paper, Nuclear Integrated Safety System (NISS) is introduced. NISS is composed of physically integrated tripe system and Interfaces among 4 safety systems are integrated.

2. Conceptual Design of NISS

2.1 Multiplexed Structure

In common with existing safety system [1~4], 4 channels are configured but in one channel, physically integrated multiplexed structure is configured in NISS. And In channel, multiplexed structure is dual and triple system, considering safety and economics. The modules that require judgment, decision of system level are configured triple system in case of detected failure and undetected failure. And the module s that are relation to interface, not require judgment and decision are configured dual system. Namely, NISS is combined dual system considering detected failure and trip system considering undetected failure. Reconfiguration by detected failure is applied to the component level modules that include power, communication, and bus module. Filtering to prepare fail of detection failure is applied to system level modules that include a processor, input/output module.

2.2 Treatment of Failure

Detection method of failure for a treatment of failure is the forwarding error detection. This is, a process module detects failure of input module, a receiving module detects failure of bus, communication module and an output module detects failure of process module. The purpose of multiplexing in a channel is to enhance availability thus if failure of one group in a channel happens, fail –disable is applied to system not fail-safe. For example, if triple output module that receive data from triple processor module detects failure of one process module, normally operates using two processor modules not to for fail-safe be applied to system. Only if uncertainty of decision exits, fail-safe is applied to system, namely if result data of two processor module is different from each other, fail-safe is applied to system.

Reconfiguration of dual system that includes bus, communication module uses primary/Hot-standby method, this is, if failure of primary module is detected, hot-standby module is used. Input/output module that is configured to triple system uses 2/3 voting logic in digital value and uses mid-value in analog value. Only average value of two values is used, if failure of one module is detected and the average value must exist in margin of error. If the average value does not exist in margin of error, fail-safe is applied to system. Table I is example for treatment of failure.

Table I: Method of treatment failure of processor module for triple input module

Digital(Discrete)			
Detect or undetected failure	**Number for failure module**	**Input**	**Decision**
Un-detection of failure	N/A	N/A	2/3
Detection of failure	1	Same state	Same state value
		Different state	Safe-Actuation
	2	N/A	Value of not fail module
	3	N/A	Safe-Actuation
Analog(Continuous)			
Detect or undetected failure	**Number for failure module**	**Number for failure module**	**Number for failure module**
Un-detection of failure	N/A	N/A	Mid value
Detection	1	Deviation <Error	Average value
		Deviation >Error	Fail

of failure	2	N/A	Value of not fail module
	3	N/A	Fail

2.3Configuration of module

Communication module of NISS is configured to two networks (safety critical network, safety related network) and independence is maintained. Each communication module uses dual system of primary/hot-standby in case of single failure. Protocol in communication module is deterministic. Effective transmission rate is 20Mbps and topology is star. Bus of NISS uses serial bus, and dual system of primary/hot-standby in case of single failure. Bus is configured to two buses. The one is for data interface of safety critical network and the other is for data interface of safety related network. Input/out module is configured to triple system. Each module has decision logic.

2.4 Interface

Interface among RCOPS, RPS, ESF-CCS, QIAS-P is integrated one network. MTP/ITP is configured to physically and functionally integrated structure. Interface between channels is peer to peer, no handshaking method. Block diagram of NISS is Fig.2. Input/output module and processor module are configured to triple system. And bus, communication module and processor module in loop controller are configured to dual system. Process variable is transmitted to triple input module. Each module validates input value and transmits data to triple processor module in dual bus Each BP uses primary bus, if failure of primary bus and hot-standby bus is not detected or failure of hot-standby bus is detected. And if failure of primary bus is detected, hot-standby bus is used. If value of triple input is digital value, 2/3 voting logic is applied, and if value of triple input is analog value, mid value is applied. Resulting data by BP is transmitted to triple CPs through dual communication system. Triple CPs use primary communication modules, if failure of primary communication and hot-standby communication is not detected or failure of hot-standby communication is detected. And if failure of primary communication is detected, hot-standby communication module is used. CP performs 2/3 voting logic for itself channel and 2/3 voting logic for other channel. Triple GCs also receives the resulting data from triple CPs through dual communication, and perform 2/3, 2/4 voting logic. Dual LCs receives the resulting data from triple GCs, and perform 2/3 voting logic. Finally the resulting data is transmitted to CIM

3. Conclusions

In this paper, conceptual design of NISS is introduced. Multiplexing method of NISS is combined dual system with triple system. Dual system includes power, bus, communication module, and triple system includes input/output, processor module. Treatment of failure uses forward error detection method. Interface among RCOPS, RPS, ESF-CCS, QIAS-P is integrated one network. And MTP/ITP is configured to physically and functionally integrated structure.

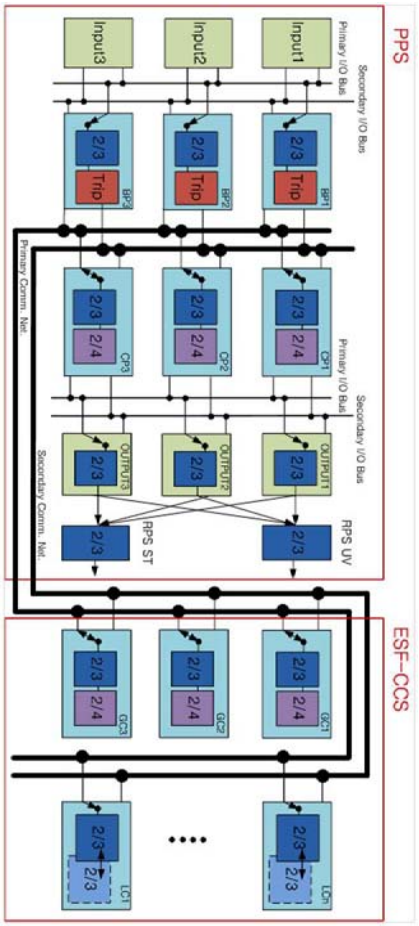

Fig. 2. Block diagram of NISS

REFERENCES

[1] Design specification for plant protection system (Shin-Kori units 3 and 4), Rev. 03, KEPCO E&C
[2] Design specification for engineered safety features-component control system (Shin-Kori units 3 and 4), Rev. 02, KEPCO E&C
[3] Design specification for plant protection system (Shin-Ulchin units 1 and 2), Rev. 02, KEPCO E&C
[4] Design specification for engineered safety features-component control system (Shin-Ulchin units 1 and 2), Rev. 01, KEPCO E&C

ACKNOWLEDGMENT
This work was supported by the nuclear Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning(KETEP) grant funded by the Korea government Ministry of Knowledge Economy
(No. 2010161010001G)