Journal of the Korean Nuclear Society
Volume 28, Number 4, pp. 359~365, August 1996

Feasibility Study on KSNP Adaption of French Digital Protection System

Jun Mo Koo, Young Ryul Lee, Ho Chang Jung, Ik Ho Chang, and Jai Bok Han

Korea Atomic Energy Research Institue
150 Dukjin-dong, Yusong-gu, Taejon 305-353, Korea

(Received October 4, 1995)

Abstract

Upgrade of nuclear power plant I&C systems by using digital technology has been implemented to overcome the obsolescence of existing equipment and improve plant availability in many advanced countries. For upgrade of the Plant Protection System(PPS) based on conventional analog technology in the UCN 3&4 and YGN 5&6, French modernized Digital Integrated Protection System(DIPS) with proven technology is reviewed and evaluated for the adaptability into PPS. This paper contains the results of feasibility study for the design of digital PPS using French DIPS technology. Based on the results of evaluations, the system architecture of digital PPS is designed and described.

1. Introduction

Upgrade of nuclear power plant I&C systems by using digital technology has been implemented to overcome the obsolescence of existing equipment and high maintenance costs due to aging components in many advanced PWR plants. In addition, the use of modernized digital technology allows of improving plant reliability and safety. KSNP(Korean Standard Nuclear Power Plant) PPS based on UCN 3&4 was designed with conventional analog technology and is to be placed in the same situations. KAERI has established the upgrade plan of PPS in order to cope with these problems. For upgrade of the Plant Protection System(PPS), the feasibility study for the adaptation of French Modernized I&C technology(hereinafter MP'4) to PPS was performed by KAERI and Framatome. This report describes the results of feasibility study to digitalize Plant Protection System using MP'4, which is Digital Integrated Protection System performing the functions of Plant Protection System, Core Protection Calculator System(CPCS) and ESFAS-ARC in the KSNP. As a reference plant of MP'4, N4 DIPS is reviewed and evaluated for adaptability of PPS. This study contains an overview of N4 DIPS, and the evaluations in accordance with KSNP requirements. For the CPCS, adaptability for integrating CPCS into PPS is evaluated. The differences between 4 and different 8 reactor trip breakers are also evaluated in view of trip safety. Finally, the new architecture of digital PPS is proposed based on evaluation results, and functional descriptions are provided.

2. Overview of N4 DIPS

The N4 DIPS is the integrated protection system, so all reactor trip functions include high LPD, low DNBR and all ESF functions. The DIPS structure is shown in Fig. 1, and it is composed of four channels

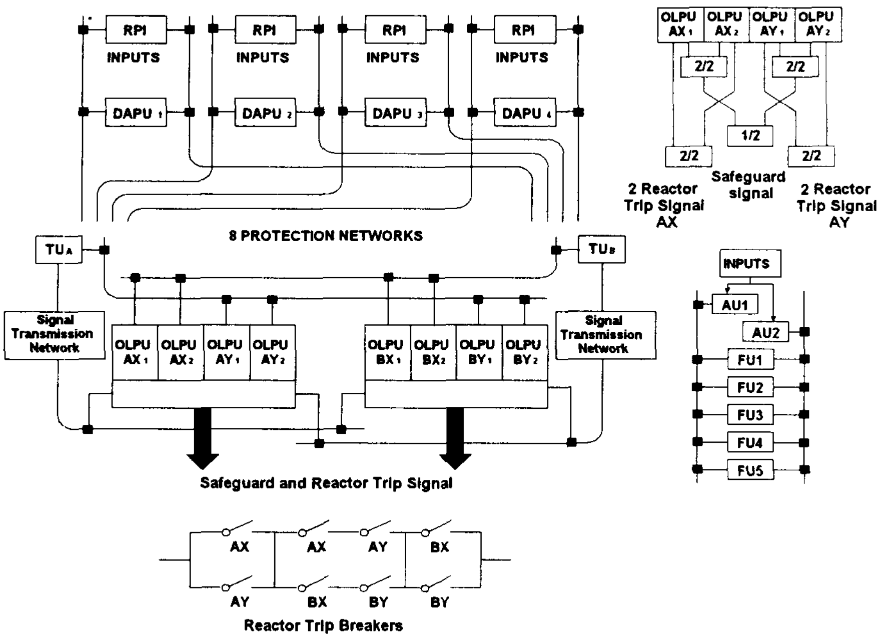


Fig. 1. Architecture of N4 Digital Integrated Protection System

of DAPU (Data Acquisition and Processing Unit), two channels of OLPU (Output Logic Processing Unit), one CTU (Central Test Unit), four LPTUs (Local Protection Testing Unit) for DAPU, two LPTUs for OLPU, four Protection Networks and two Signal Networks, and two channels of DTU (Diagnostic and Transfer Unit).

The OLPU consists of OLPU A and B. The OLPU A contains logic AX and AY, and each contains two PPUs performing 2/4 logic. The DAPU receives the trip signals by redundant Acquisition Units(AUs), performs trip setpoints and calculations in the Functional Units(FUs), and sends trip signals to OLPU through networks. OLPU performs the acquisition of the signals from DAPU on the protection networks and logic processing, and initiates reactor trip order and engineered safeguard orders. Each OLPU is composed of four PPUs which are regrouped 2 half logic (X and Y) and one LPTU. In each half logic, one PPU receives the information of FUs through one protection networks and other PPUs receive the information of FUs through the opposite network. Each PPU receives and transmits the information on two signal networks. Safeguard action commands coming through two PPUs of same 1 out of 2 logic are regrouped to perform the AND function of actuator cards. In the DIPS, two types of network are implemented, one is NERVIA network with token pas sing bus type and the other is actuator network with master-slave protocol. The NERVIA networks are composed of 10 networks; 8 protection networks and 2 signal networks. The DTU performs the transfer of information, the operator interface, the maintenance and the diagnosis of the DIPS malfunction.

3. Evaluations For DIPS Adaptation Into PPS

Codes, Standards and design requirements used in the UCN 3&4 are retained for the design consistency and to minimize licensing impacts and the interface problems between the I&C systems and other systems. The N4 DIPS as a reference plant of MP'4 is reviewed, and so this section contains the evaluations to review if N4 DIPS can be adapted into KSNP in accordance with the KSNP design requirements. Also, adaptability of CPCS into DIPS is evaluated, and four and eight reactor trip breakers are evaluated in view of trip safety. The following evaluation are performed.

a) Safety Design Requirements

PPS and DIPS are class 1E safety systems and seismically qualified. The computerized workstations and auxiliary panels for N4 are non-safety systems. The redundancy of receiving two input signals in one channel is implemented for fault tolerant design. For DIPS architecture, DAPUs which receive input signals and calculate a variety of trip setpoint are composed of 4 channels, but OLPUs which perform 2 out of 4 logic and the initiation of reactor trip and ESF functions are composed of two trains. So the architecture of OLPU is needed to be modified with 4 independent channels to meet the separation requirement.

b) Defence Against Common Mode Failure

The use of computer software could result in a common mode failure. Diversity is one method of addressing this concern according to IEEE 7.4.3. 2-1993. In the DIPS, functional diversity is achieved with four(4) fold redundancy to protect a single and common mode failure. The diverse parameters for DIPS are processed in different functional units (FUs), so reducing consequently the probability of failure of the protection function due to a common cause. If one functional unit fails to generate the trip signal for preventing core damage accident, other functional units can generate the redundant trip signal for same accident. Also IEEE 7.4.3.2-1993 describes that diversity is not required if Anticipated Transient Without Scram system or manual operator action is provided. Therefore common mode failure is considered that it is not a concern since diverse protection system for ATWS and manual operation are provided in the KSNP.

c) Control, Alarm, Test and Bypass Function

DAPU performs the generation of turbine runback and CEA Withdrawal Prohibit(CWP) by DNBR and LPD signal, and CWP by neutron flux, but the CWP for PPS is generated from high pressurizer pretrip and CPC/CWP signals. In order to meet PPS requirements, the provision for only CWP function shall be implemented. For operating bypass, the signal for adjusting the trip setpoint by the operator shall be transmitted to the AUs.

d) Remote Control Module (RCM) Function

There are two modules such as PPS remote control module and CPC operator's module, which are the class 1E equipment and located in the main control room(MCR), and these equipments are composed of 4 channels independently, and provided with mechanical and electrical isolation. But there is no class 1E equipment in N4 MCR. In order to meet this requirement, the class 1E signal connections by wire to wire from OLPU to remote control module and from DAPU to operator's module shall be implemented instead of non-classified DTU.

e) Networking

NERVIA network used in the DIPS is a real time oriented communication of serial type links, and deterministic access protocol, token ring, diffusion type network is used. NERVIA permits two way communication between the upstream station and downstream stations. However, downstreams cannot communicate among themselves to provide a point of software isolation.

The NERVIA networks are composed of 8 protection and 2 signal networks. Protection networks are safety class, but signal networks are non-safety. The interfaces to and communication between DIPS and plant computer system is designed with buffering fiber optic to ensure electrical isolation. Gateway is implemented with a serial data link using a standard protocol in accordance with Utility Requirements Document Chapter 10. Therefore, NERVIA networks meet the communication independence defined in Annex G of the IEEE 7.4.3.2-1993.

f) Software Qualification

The Software development procedure for class 1E software complies with a software quality assurance plan (SQAP) and IEC 880 in the DIPS. Software V/V activities are performed by independent V/V groups at each stage. Designers perform verification and tests of software internal calculations prior to delivering software to the verifiers. Once one particular step of the software development cycle has been completed, a design review is organized prior to the following step. Verification (including preparation of test input/output, verification of software design and coding, test execution) is performed by engineers other than those involved in software design and generation. Test results are documented and detected errors are reported. Verification and tests are then again carried out as necessary. Software development procedure complies with "V" cycle and each phase of cycle is as follows: System Specification, Software Specification, Preliminary Design, Detailed Design, Coding, Module tests, Integration Tests, Validation tests, Interconnection Tests, On-site Tests, Operation. The software qualification is performed during the downward phases of the cycle to avoid introducing errors, and is observed during the upward phases of the cycle (test and validation) to detect remaining errors. French V/V procedure is similar with one used in the PWR, and France has V/V experiences over 15 years. For the digital PPS, all software activities will be met in accordance with IEEE Std 7-4.3. 2-1993. Since IEEE Std. 7.4.3.2 refers to IEC Std. 880, it would not be concerns.

g) Evaluation of CPCS

Implementation of CPCS into PPS may require a lot of manpowers. Two cases are considered for both the implementation of CPCS into PPS and the separation of CPCS from PPS. The functions of the CPCS can be implemented in the DIPS with addition of CEAC processor and Operator's Module processor. For CEAC which monitors all CEA positions in the core and detects deviation in the subgroup, additional units will be required. So Interface Functional Unit(IFU) will perform the functions of CEAC. In this case, the interfaces with other I&C systems can be simplified with the use of networks. The application of Computer Aided Software Engineering (CASE) tool SAGA enhances the reliability of the system by reducing any human errors or mistakes to be introduced in the design, and it can reduce equipment cost and manpower in the process of software V/V. But with use of same tools and processors, common mode failure might be more susceptible. The fact that DIPS is not the off-the-shelf equipment makes it difficult for future upgrade and to maintain spare parts.

h) Evaluations of Reactor Trip Breaker System

In the N4, eight reactor trip breakers are implemented in such a way that 2/4 logic initiates four pairs of two breakers. In the KSNP, four reactor trip breakers are implemented. Simultaneous failures of selective two channels such as either fail closure of PPS initiation relays or breakers in the channels A/C or B/D result in trip failure. In the N4, the structure of DIPS enables it to withstand double failures. Two channels failures will never initiate reactor trip due to extensive use of the 2/4 logics. In failure of two pairs of trip breakers, reactor can be tripped by other breakers. Also extensive use of 2/4 logic in the breaker arrangement prevents any trip initiation demand to fail and any spurious initiation to occur in case of a single failure even when one channel is in maintenance. Therefore eight trip breakers using general 2/4 logic can improve the trip safety and plant availability during the maintenance.

As a result of evaluations, some modifications of N4 DIPS are required. For the function of adjusting trip setpoint, the hard-wired connections from RCM and RSP to AUs are provided. For the functions of CPCS, the additional AUs, EU, IFU, and LPTU are provided, and also the exchange networks are provided to communicate with these additional equipments. The provision for class 1E connection between DIPS and MCR is provided.

4. Design of Digital Protection System

Based on the evaluations per section 3.0, the new system architecture for digital PPS is proposed and described. The proposed architecture for digital PPS is shown in Figure 2 and 3. The proposed PPS consists of four channels of DAPU, OLPU and two channels of DTU. In order to improve the system reliability, eight reactor trip breakers are required and wired in such a way that 2/4 logic is obtained from sensors to reactor trip breakers. The followings describe the function of major components of digital PPS.

a) DAPU Cabinet

Each channel of DAPU A and B is composed of 2 AUs, 5 FUs, 1 local test unit, and 1 additional Exchange Unit (EU), and each channel of DAPU B and C is composed of 2 AUs, 5 FUs, 1 LPTU, and 2 additional AUs, 1 LPTU, 1 EU and 1 IFU. Two AUs in each channel receive the input signals and transfers the conditioning signals to FUs via the protection networks. The functions of EU are to send the rod position signals inputs to other channels, and to receive the penalty factor from Interface Functional Unit (IFU), and EUs are connected to operator's module and class 1E indicators of excore instruments in the MCR. To perform the function of adjusting trip setpoint for low Pressurizer Pressure and Low Steam Generator Pressure, the connection from remote control module and from RSP to AU by wire to wire is provided. The additional exchange networks are provided. This network is used to communicate between EUs and IFUs. Five FUs in each channel which calculate the reactor trip and ESFAS signals perform the setpoint calculation in accordance with functional diversity. Safety analysis is required to assign trip parameters in the FUs later.

b) OLPU Cabinet

The OLPU generates ESFAS signals and reactor trip signals from four DAPUs, from logic inputs of the process instrumentations, or from main control room. It provides functional alarms in hard-wired outputs for the control room and sends data to the DTUs. OLPU contains two PPUs which perform auctioneering and processing required to combine signals, and transmits the safeguard action and reactor trip signals. One OLPU initiates two trip breakers, and contains a local test unit performing periodic testing. The provision for the class 1E connection between remote control module and OLPU is implemented by wire to wire. The manual actuation and reset signals from MCR for Remote Shutdown Panel(RSP) and ESFAS are directly connected to OLPU and also remote manual MSIS signal from RSP is directly connected to OLPU. One PPU communicates with a reactor trip card and safeguard action cards through the actuation device networks. It performs 2/4 logic from four DAPU to processes signals transmitted by each Functional Unit.

c) DTU and Central Test Unit(CTU)

This cabinet performs the non-class 1E communication between DIPS and other I&C systems via the protection and signal networks. CTU performs the periodic test for proposed architecture. In addition, the functions of status panels for maintenance and test in the PPS cabinet are included in the CTU.

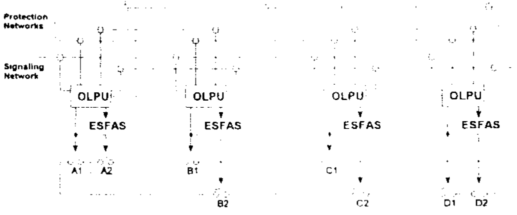


Fig. 2. Overall Architecture of Digital PPS

d) Remote Control Module

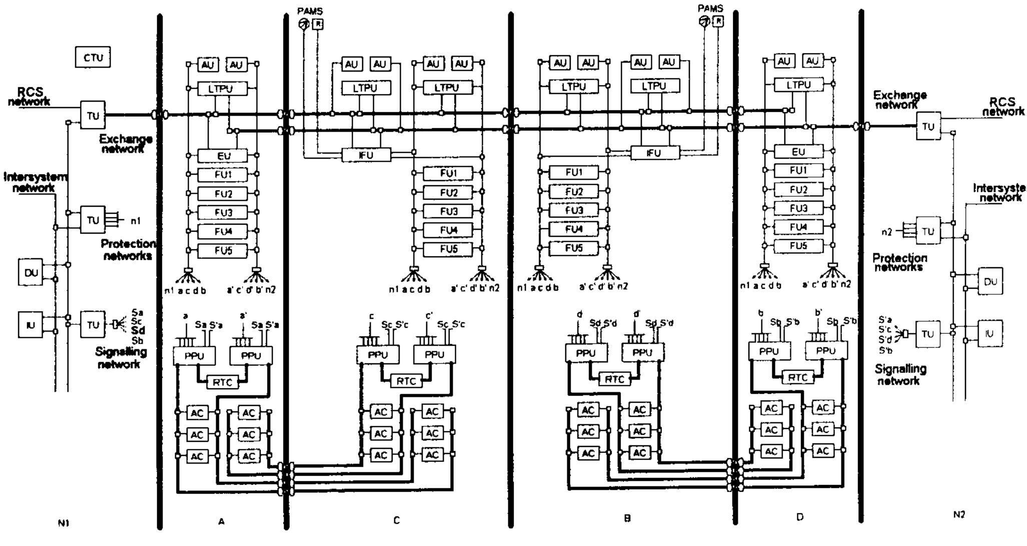
Remote Control Module is composed of 4 channels of class 1E equipment in MCR. Operator's module is connected to EU and OLPU by wire to wire. This module is connected to AU and OLPU by wire to wire and the functions of this module are information for pretrip and trip, bypass for low pressurizer pressure trip, bypass for high log power trip, setpoint reset for low pressurizer pressure trip, setpoint reset for low steam generator pressure trip.

5. Conclusions

In this study, French modernized DIPS of proven technology is reviewed and evaluated for the adaptability into KSNP PPS. Based on the result of evaluations, some modifications of N4 DIPS are required, and the proposed architecture of digital PPS is prepared. For the function of adjusting trip setpoint, the hard-wired connections from RCM and RSP to AUs are provided. For the functions of CPCS, the additional AUs, EU, IFU, and LPTU are provided, and also the exchange networks are provided to communicate with these additional equipments. The provision for class 1E connection between DIPS and MCR is provided. CPCS integration into DPPS requires further evaluation. Eight reactor trip breakers system is recommended in view of trip safety instead of four reactor trip breakers. However, it may be subject to change depending on target of overall reliability of digital PPS. Digital PPS is expected to provide the improvements of plant safety, reliability and testability. It is expected that the results of this study could be applied for Future Nuclear Power Plant.

Acknowledgements

The authors would like to express thanks to A. Parry, T. Zumbihl, F. Dionis who worked jointly at Framatome for this study. The authors also wish to thank D.S. Kim and B.R. Lee (KAERI) who support for this study in the project aspects.



AC : Actuator Card
AU : Acquisition Unit
DU : Diagnosis Unit

EU : Exchange Unit
FU : Functional Unit
IFU : Interface Functional Unit

IU : Interface Unit
LTPU : Local Testing Protection Unit
PAMS : Post-Accident Monitoring System

PPU : Protection Processing Unit
RTC : Reactor Trip Card
TU : Transfer Unit

Fig. 3. Detailed Architecture of Digital PPS

References

1. KAERI/IM-217/93, "Feasibility Study for KSNP Adaptation of Advanced I & C System in the French Nuclear Power Plant"
2. System Description of PPS For UGN 3 and 4, N0291-SD-560.
3. Dossier de Systeme Elementaire ; System de Protection de Reacteur, Rev. C, IN/L-DC-0073, 22 July 94, Framatome.
4. Guide d'Exploitation et d'Entretien ; System de Protection Integre Numerique, Rev. B, May 93, Merlin Gerin.
5. A. Parry, "Advanced I&C System For Nuclear Power Plants", Framatome, Presentation Material (1992)
6. KAERI/AR-412/94, "A Survey on the Development of Advanced Instrumentation and Control System in the Nuclear Power Plant"
7. M. Bruyere, "Operating Experience of An Advanced Protection System On French 4 Loop Plants", German Atom Forum, Federal Republic of Germany(1986)
8. E.W. Hagent, "Common-Mode/Common Cause Failure", Vol. 21, No. 2, Mar (1980)
9. IEC Std. 880/1986, "Software for Computers in the Safety Systems of NPP"
10. IEEE Std. 7-4.3.2/1993, "Criteria For Digital Computers in Safety Systems of NPP"
11. G. Ives, Digital systems : Reviews of Safety Critical Applications, Instrumentation and Control, Nuclear Engineering International, Apr (1994)
12. T. Albrigo Warning : Digital Systems Ahead, Instrumentation and Control, Nuclear Engineering International, Apr (1994)