TECHNICAL REVIEW ON THE LOCALIZED DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

KEE-CHOON KWON* and MYEONGSOO LEE[1]
Korea Atomic Energy Research Institute
[1]Korea Electric Power Research Institute
*Corresponding author. E-mail : kckwon@kaeri.re.kr

Invited February 11, 2009
Received March 31, 2009

This paper is a technical review of the research and development results of the Korea Nuclear Instrumentation and Control System (KNICS) project and Nu-Tech 2012 program. In these projects man-machine interface system architecture, two digital platforms, and several control and protection systems were developed. One platform is a Programmable Logic Controller (PLC) for a digital safety system and another platform is a Distributed Control System (DCS) for a non-safety control system. With the safety-grade platform PLC, a reactor protection system, an engineered safety feature-component control system, and reactor core protection system were developed. A power control system was developed based on the DCS. A logic alarm cause tracking system was developed as a man-machine interface for APR1400. Also, Integrated Performance Validation Facility (IPVF) was developed for the evaluation of the function and performance of developed I&C systems. The safety-grade platform PLC and the digital safety system obtained approval for the topical report from the Korean regulatory body in February of 2009. A utility and vendor company will determine the suitability of the KNICS and Nu-Tech 2012 products to apply them to the planned nuclear power plants.

KEYWORDS : Programmable Logic Controller, Digital Safety System, Distributed Control System, Power Control System, Simulator, Integrated Performance Validation Facility

1. INTRODUCTION

The major functions of the Instrumentation and Control (I&C) in Nuclear Power Plants (NPPs) are monitoring, control, and protection which are similar to the functions of the brain and neural network in a human body. During their extensive service history, analog I&C systems have performed their intended monitoring and control functions satisfactorily. Although there have been some design problems, such as inaccurate design specifications and susceptibility to certain environmental conditions, the primary concerns with the extended use of analog systems are the effects of aging, such as mechanical failures, environmental degradation, and obsolescence.

The industrial base has largely been switched to digital-based systems. The reason for the transition to digital I&C systems lies in their important advantages over existing analog systems. Digital electronics are essentially free of the drift that afflicts analog electronics, so they maintain their calibration better. They have an improved system performance in terms of accuracy and computational capabilities. They have higher data handling and storage capacities, so operating conditions can be more fully measured and displayed [1].

Korea has twenty NPPs under commercial operation, six plants under construction, and also has a plan to construct two new nuclear power plants by 2016. Korea ranks as the sixth largest country in the world for having its annual electric power generated by NPP, but we did not have our own I&C systems. In order to achieve technical self-reliance in the area of nuclear I&C, the KNICS project and Nu-Tech 2012 program had been running for several years. Research institutes, engineering companies, manufacturing companies, venture companies, and universities have participated in the KNICS and Nu-Tech 2012 Research and Development (R&D) program. The final goal of the projects is to apply the R&D results to the APR1400 Man-Machine Interface System (MMIS).

The APR1400 MMIS architecture was originally designed by the Korean Next Generation Reactor (KNGR) project. The MMIS architecture hierarchically consists of three layers to meet the design requirements of the APR1400 that was design certified by the Korean regulatory body in 2002. The top level consists of a control room, an information processing computer system, and an indication system. The control system and protection system are located in the middle level. The bottom level consists of the measurement systems for the various

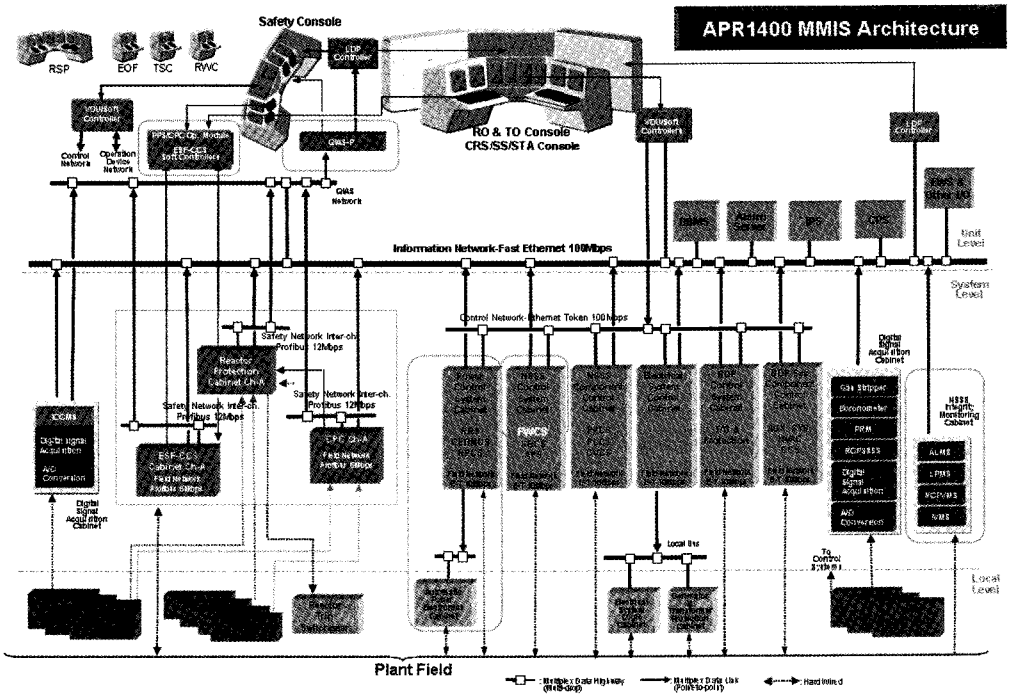

Fig. 1. APR1400 MMIS Architecture

equipments. Networks are widely used for the intra-system and inter-system connections in the MMIS architecture. Figure 1 shows the APR1400 MMIS architecture [2,3].

2. DIGITAL I&C SYSTEMS

2.1 Programmable Logic Controller

The safety-grade Programmable Logic Controller (PLC) platform named POSAFE-Q was developed so that it meets the requirements of the Safety Class 1E, Quality Class 1, and Seismic Category I.

The PLC consists of various modules such as a power module, a processor module, communication modules, digital input/output modules, analog input/output modules, a local bus extension module, and a high-speed pulse counter module. The PLC installs two independent power modules in a rack. 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 PLC operation. The PLC can extend the number of input/output module through a local bus extension module. The communication modules consist of Profibus-Fieldbus Message Specification (FMS), High Reliability-Safety Data Link (HR-SDL), and High Reliability-Safety Data Network (HR-SDN). The Profibus-FMS module for information communication is classified as safety related, the HR-SDL for peer-to-peer communication is classified as safety critical, and the HR-SDN is for the safety critical network.

The processor module uses a Texas Instrument DSP CPU and the real-time operating system named pCOS was developed based on the Micro-C real-time operating system. All communication modules were developed based on the Field-bus protocol to meet the deterministic requirements. The RS-485 and RS-422 for serial communications are also supplied.

The engineering tool named pSET was also developed. The developers of the application programs can perform programming, debugging, and simulation on the pSET environment. The application program developed on the pSET is downloaded into the processor module through RS-232C. The pSET operates on Windows 2000/NT, which meets the IEC 61131-3 requirements. Figure 2 shows the configuration of the developed PLC [2,3].

All the software and firmware of the POSAFE-Q PLC were developed and verified following the software development life cycle Verification and Validation (V&V) procedure. The main activities of the V&V process are preparation of software planning documentations, verification of the Software Requirement Specification (SRS), Software Design Specification (SDS) and codes, and a testing of the software components, the integrated software, and the integrated system. In addition, a software safety analysis and a software configuration management are included in the activities.

The SRS V&V activities consist of a technical evaluation, a licensing suitability review, an inspection

and a traceability analysis, a formal verification, preparation for an integrated system test plan, a software safety analysis, and a software configuration management. Also, the SDS V&V activities include a technical evaluation, a licensing suitability review, an inspection and traceability analysis, a formal verification, preparation for an integrated software test plan, a software safety analysis, and a software configuration management. The code V&V activities include a traceability analysis, a source code inspection, a component test case, a test procedure, and a test report generation, a software safety analysis, and a software configuration management. Testing is the major V&V activity of the software integration and system integration phase. Software safety analysis at the SRS and SDS phases uses the Hazard Operability (HAZOP) method, and at the implementation phase the source code has been evaluated using the safety programming guide of NUREG/CR-6463. Finally, the software configuration management was performed using the Nuclear Software Configuration Management (Nu-SCM) tool developed in the KNICS project [4,5].

2.2 Reactor Protection System

The Integrated Digital Protection System (IDiPS) is a plant protection system that includes a Reactor Protection System (RPS), an Engineered Safety Feature-Component Control System (ESF-CCS), and a Reactor Core Protection System (RCOPS). The IDiPS RPS generates a reactor trip signal and the engineered safety feature actuation signals automatically whenever the monitored processes reach the predefined set-points.

The IDiPS RPS is designed with a redundant 4-channel architecture, and every channel is implemented with the

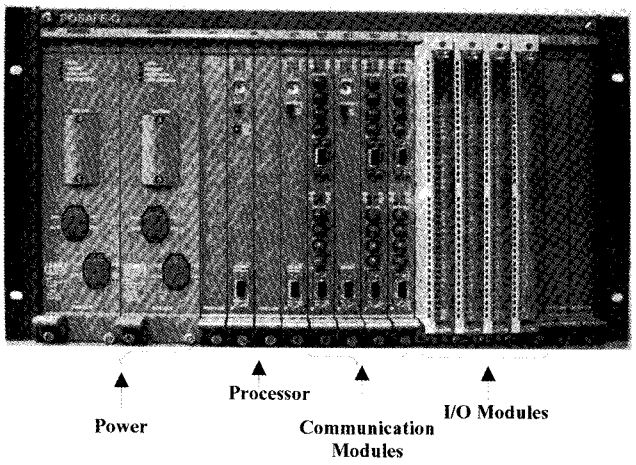

Fig. 2. POSAFE-Q PLC

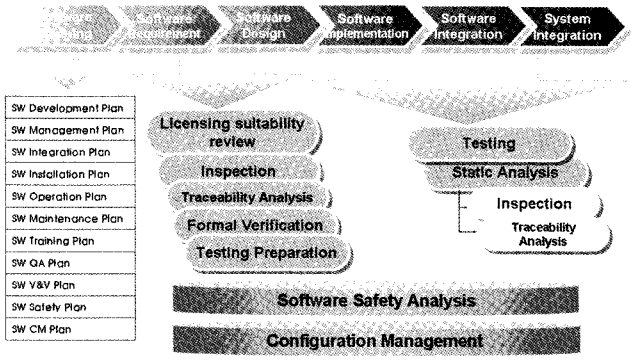

Fig. 3. Software V&V Activities

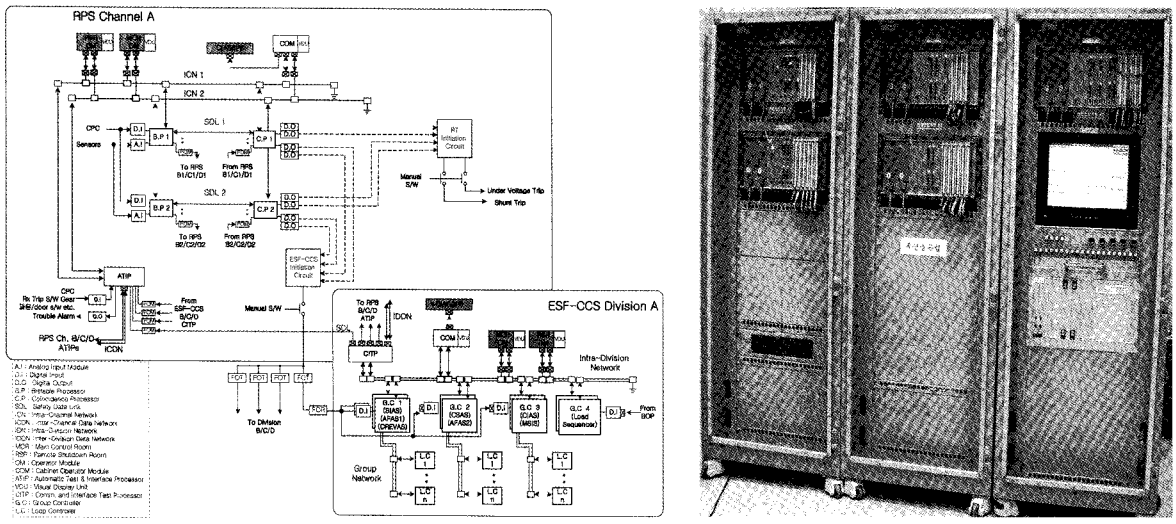

Fig. 4. Architecture of One Channel IDiPS RPS and Prototype

same architecture. A single channel consists of a redundant Bi-stable Processor (BP), a redundant Coincidence Processor (CP), an Automatic Test and Interface Processor (ATIP), and a Cabinet Operator Module (COM). The BP module generates a logic-level trip signal by continuously comparing the sensor inputs with the predefined trip set-points. The logic-level trip signals generated in the BP module of each channel are transferred to the CP modules of all the channels via the HR-SDL. The CP module monitors the logic-level trip signals transferred from the four BP modules. When two or more logic-level trip signals from the BP channels are activated, the CP modules will activate the output signal for the reactor trip. The ATIP module monitors the operation status of the IDiPS RPS, and conducts the surveillance test to ensure a reliable operation of the BP and the CP module in the same channel. The test results of the ATIP are transferred to the COM module that has an operator interface facility implemented with an industrial PC and a flat panel display. The BP, CP, and ATIP modules of the RPS were implemented with the POSAFE-Q PLC platform. Figure 4 shows a single channel architecture of the IDiPS RPS and its prototype [2,3].

2.3 Engineered Safety Feature-Component Control System

The IDiPS ESF-CCS initiates several emergency actuations to prevent a plant in a hazardous state during and/or after accidents. The actuations include a safety injection, a containment isolation, a main steam line isolation, an auxiliary feedwater injection, and a containment spray actuation.

The IDiPS ESF-CCS is designed with four redundant divisions (i.e., A, B, C, and D), and implemented with the PLC platform. The principal components of an individual division are fault tolerant Group Controllers (GCs), Loop Controllers (LCs), an ESF-CCS Test and Interface Processor (ETIP), a COM and a Control Channel Gateway (CCG).

Each GC receives ESF initiation signals from the RPS and radiation monitoring system via fiber-optic receivers. All GCs perform a system level nuclear steam supply system and balance of plant ESFAS logic independently, so that they can transfer the system level ESF actuation signals to all LCs in the division. LCs perform a component control logic using system level ESF actuation signals from GCs or component level control signals from an operator, so that the output control signals are assigned to individual plant components. ETIP takes charge of the passive and active test functions of the ESF-CCS and the interfaces of the ESF-CCS with other systems such as the RPS and qualified indication and alarm system. COM provides information about an ESF actuation status, an ESF component status, a module status, and so on. CCG supports the interface between the ESF-CCS and ESF-CCS soft controllers in the main control room or remote shutdown room. Figure 5 shows the configuration of division A of the ESF-CCS and developed prototype [2,3].

2.4 Reactor Core Protection System

The core protection calculator system provides on-line calculations of the Departure from Nucleate Boiling Ratio (DNBR) and Local Power Density (LPD) of the existing plant. It generates a reactor trip signal when the condition exceeds the DNBR or LPD design limit. It consists of four independent channels employing a two-out-of-four trip logic.

Doosan Heavy Industries & Construction consortium developed its own core protection calculator system named Reactor Core Protection System (RCOPS) with an improved algorithm and a different system configuration compared to the existing system. The improved algorithms of RCOPS include DNBR algorithm improvement for core thermal margin, resolution of the latching problem

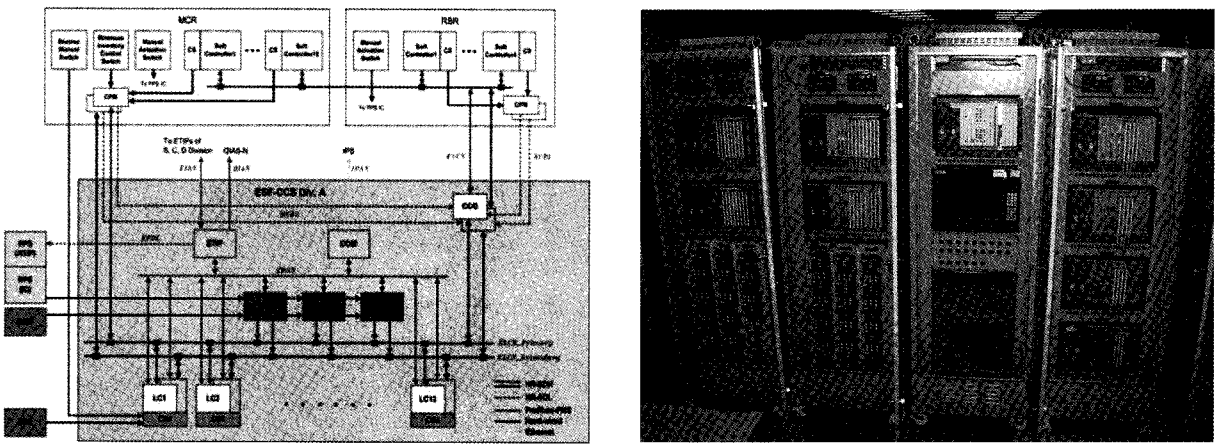

Fig. 5. Configuration of One Division IDiPS ESF-CCS and Developed Prototype

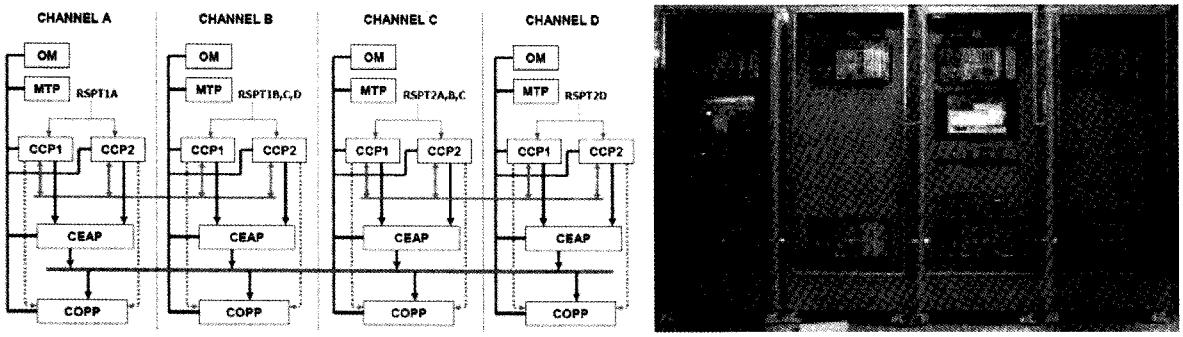

Fig. 6. Block Diagram of RCOPS and Developed Prototype

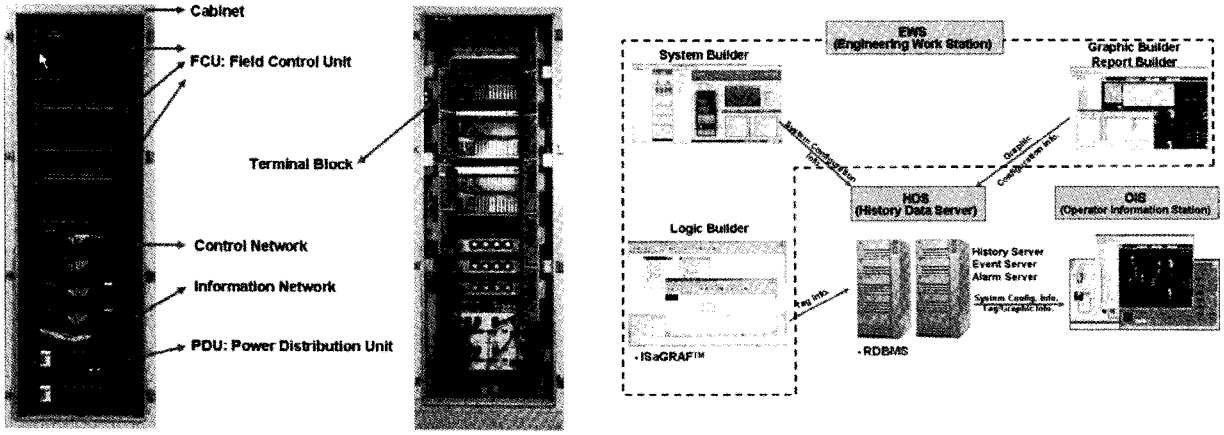

Fig. 7. Hardware and Software Structure of DCS

of the false Control Element Assembly (CEA) signal, and addition of a pre-trip alarm generation. The RCOPS is based on the POSAFE-Q PLC which is the same hardware platform for IDiPS RPS and ESF-CCS.

Each channel of RCOPS consists of a Core Protection Processor (COPP), a Control Element Assembly Processor (CEAP), and two Channel Communication Processors (CCP). COPP monitors the CEA positions of one quadrant of the reactor core. These CEAs are called the target CEA of that channel. COPP generates planar radial peaking factors that are used to calculate DNBR and LPD. CEAP takes all CEA positions of the reactor core through CCP and examines the CEA deviation between subgroup positions. If this deviation is higher than a specified value, CEAP will send the penalty factor to COPP.

Three channels of RCOPS were implemented: one channel for software development and two channels for validation test. The software test and response time test, and long-term operational validation test were performed under an I/O simulator and an Integrated Performance Validation Facility (IPVF) adopted APR1400 simulator. Figure 6 shows the block diagram and developed one channel prototype [6].

2.5 Distributed Control System Platform

Woori technology Inc. has recently completed its developmental work for a Distributed Control System (DCS, OPERASYSTEM^{TM}) to be used in NPPs. The DCS will be used as a platform for non-safety control systems. They created this program by firsts determining the specific requirements for application of a DCS to nuclear power plants and then setting up high quality software tools to be used for this development. The developed system was tested and verified to meet the requirements for high reliability, having an integrated communication system, and for improved man-machine interfaces, as set for the APR1400 MMIS.

Figure 7 shows the hardware structure for the DCS developed for nuclear applications. The major components for this structure are the field control unit, communication network units for control signals and for information flows, and the power distribution unit. Major components of the software are Engineering Work Stations (EWS), History Data Server (HDS), and Operator Information Station (OIS) as shown in Figure 7. The EWS consists of a system builder used for configuring the system, a logic builder supporting ISaGRAF based simulation and

debugging functions, a graphic builder supporting the iFiX and ProcSee, and a report builder. The HDS utilizes a high performance relational data base management system and consists of a history server, an event server, and an alarm server. The OIS uses a communication channel for its exclusive use and can handle up to 1,000 soft control functions simultaneously.

A test plan for an integrated test and procedures for the test were developed. Necessary panels for the test were manufactured and a load test was performed including a duration test. The integration test for the DCS platform was completed successfully showing that the developed system meets all the necessary requirements set at the design stage [7].

2.6 Power Control System

A Power Control System (PCS) to be used for commercial reactors has been developed. It is applicable to any APR1400 nuclear plants that will be built in Korea. Major systems of the PCS are Control Element Drive Mechanism Control System (CEDMCS), Reactor Regulating System (RRS), and Reactor Power Cutback System (RPCS). The PCS consists of control cabinets, power cabinets, and an auxiliary cabinet as shown in Figure 8. The OPERASYSTEM™ DCS platform is applied for the systems in the control cabinet and in the auxiliary cabinet, and a processor based on a high performance digital signal processor is located inside the power cabinet to monitor and diagnose various system functions.

The PCS was designed so that the developed product will be easy to use, easy to maintain, and highly reliable. All the components have been duplicated so that the failure of a single component will not cause a drop of any control rod, hence reducing unintended power failures. Also the maintenance and test panel located inside the control cabinet provide means of storing and accessing

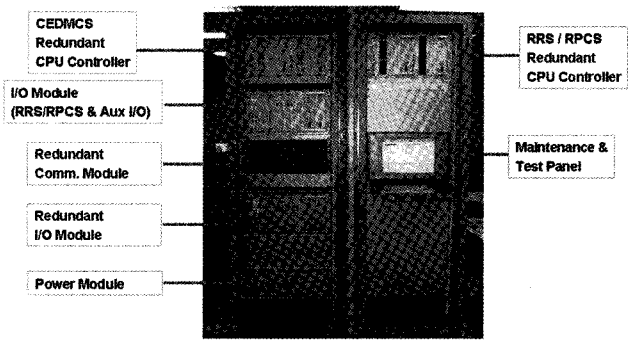

Fig. 8. Power Control System Prototype

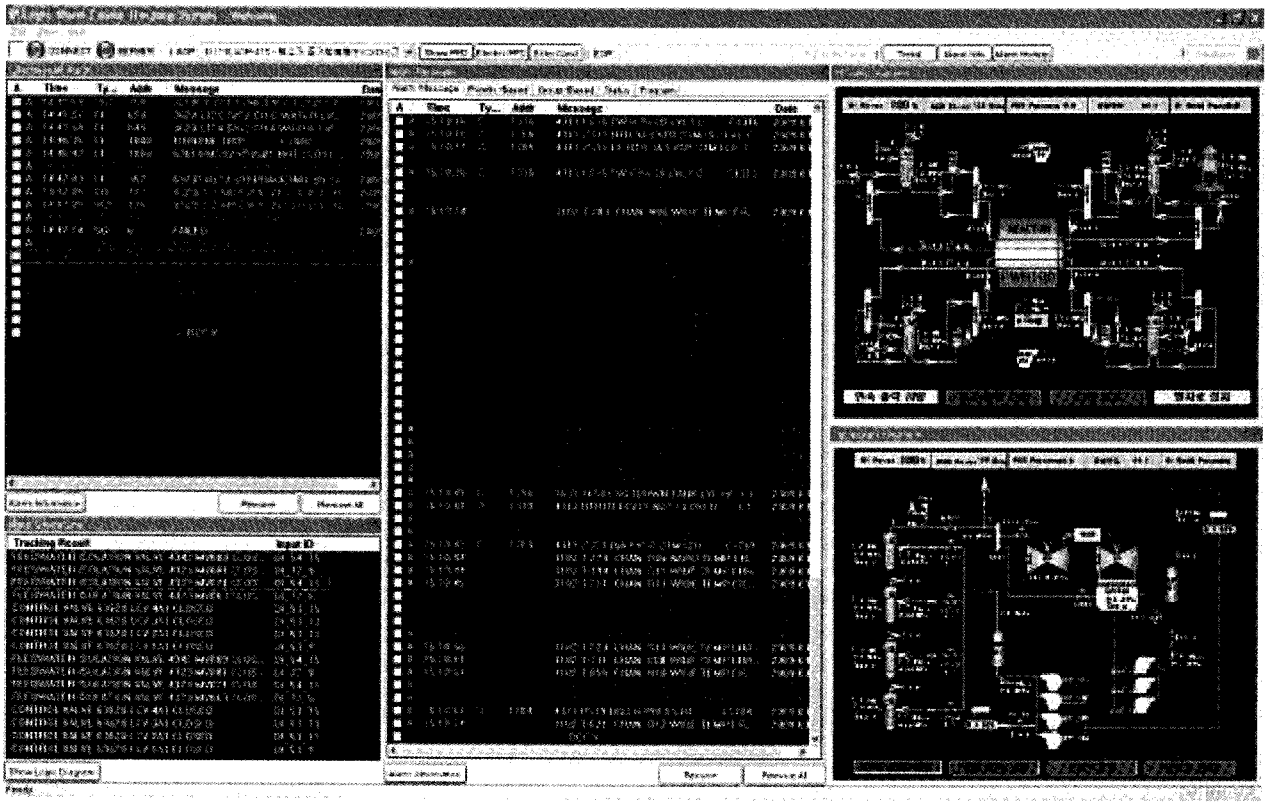

Fig. 9. LogACTS Main Display Page

various information related to not only the normal operations, but also to those events of failure. Man-machine interfaces have improved, the design was improved for better maintainability, and improvements in other areas such as monitoring, diagnosis, information displays, and data logging have also been made. For better spare parts management, the parts were selected mostly in such a way that those used in other industries will be used for the PCS. The communication between cabinets is done through a network except for some direct emergency related signal transfers, so that the cabling is minimized and the reliability is increased.

A test system was fabricated consisting of two control cabinets, one power cabinet, and one auxiliary cabinet. An integration test was performed using the test system and an equipment qualification was completed successfully. The reliability of the system has been verified by completing a 100 consecutive day test running successfully [8].

2.7 Logic Alarm Cause Tracking System

An alarm processing and presentation system called Logic Alarm Cause Tracking System (LogACTS) was developed by the KNICS project. LogACTS was developed to help the operators during transients such as setback, stepback, turbine trip, and reactor trip events.

LogACTS processes alarm messages to select important alarms among the many alarms set during the plant transients by using alarm-status separation processing, plant mode dependency processing, cause-consequence relationship processing, level precursor processing, interlock equipment processing, and common resource processing. Alarm causes were analyzed using logic diagrams, system operation procedures, and instrument drawings and then implemented into LogACTS.

LogACTS can display a list of whole alarm messages, a list of compressed alarm messages resulting from the alarm processing, the causes of an alarm selected from the list of compressed alarm messages, information of individual alarms, logic diagrams showing the result of tracking alarm causes, plant process mimic diagrams showing the status of the major components in the primary and secondary systems, and windows for checking the conditions to initiate plant abnormal operation procedures or emergency operation procedures. Figure 9 shows the LogACTS main display page.

Various features of LogACTS were verified through a prototype evaluation by plant personnel and they were validated through a pilot operation of LogACTS with data stored during previous transient events of the plant. Operators agreed that LogACTS would help them to identify the causes of plant transients and to mitigate them more easily [9].

2.8 Integrated Test and V&V of Digital I&C system

While the NPP simulators have been widely used for operator training and licensing in the nuclear industry, new emerging applications of them are spreading over many different technical fields. Some of the new important application fields are the V&V of Human Factors and Ergonomics (HFE) design of human system interaction, and the integrated performance validation of new digital control systems of NPPs.

As a design of new generation NPP, APR1400 has adapted the digital MMIS and I&C system for the plant control. The regulatory body requested the V&V step to happen in order to conform that the HFE designs enable the plant personnel to perform their tasks successfully in order to achieve plant safety and other operational goals. Korea Electric Power Research Institute (KEPRI) developed the integrated test system for an integrated system validation of APR1400 MCR design by using a full scope simulator. Figure 10 shows the configuration of the system.

Even though the KNICS I&C system, which is a localized digital I&C system by domestic companies and organizations, was developed and verified by the standards

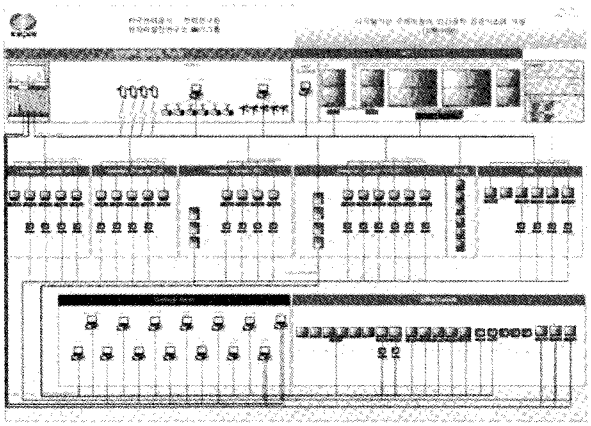

Fig. 10. Configuration of APR1400 HFE V&V System

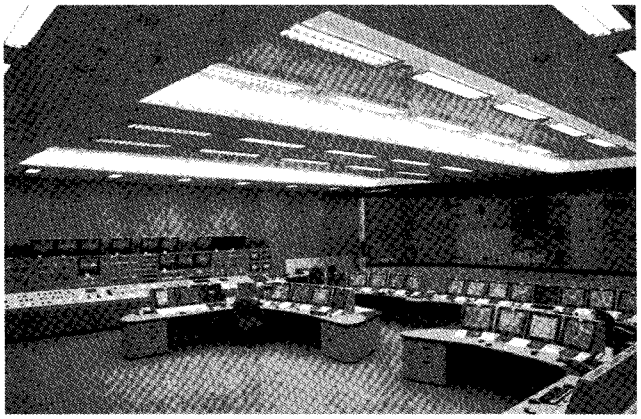

Fig. 11. Integrated Performance Validation Facility Overview

of the safety critical software and hardware design, it shall be verified soon that it satisfies the proven technology requirements for use in the NPPs I&C design. KNICS project and Nu-Tech 2012 program have developed together the IPVF that could evaluate the function and performance of all developed I&C systems. IPVF was installed in the Doosan Heavy Industries & Construction test facility, and it is being utilized to validate the developed prototype. Figure 11 shows the overview of the IPVF [10].

3. CONCLUSION

In this paper, we described a technical review on the safety-grade platform PLC, digital safety systems based on PLC, DCS platform, PCS based on DCS, logic alarm cause tracking system, and V&V facility that were developed by domestic companies or institutes. The safety-grade PLC platform and the digital safety systems, including IDiPS RPS, ESF-CCS, and RCOPS obtained the licensing approval from the Korean regulatory body via topical report. The safety evaluation reports were issued in February 2009. Utility and vendor companies will determine whether they will apply the KNICS and Nu-Tech 2012 products to the planned NPP.

REFERENCES

[1] National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, 1997.

[2] Dong-Young Lee, et al., "Development experience of digital safety system in Korea," IAEA Technical Meeting on the impact of Digital I&C Technology on the Operation and Licensing of NPP, Beijing, China, Nov. 3~6 2008.

[3] Kee-Choon Kwon, et al., "Technical Self-Reliance of Digital Safety Systems," Proceedings of the 24th KAIF/KNS Annual Conference, pp.469-474, Seoul, Korea, April 8-10, 2009.

[4] Gee-Yong Park, et al., "Fault Tree Analysis of KNICS RPS Software," Nuclear Engineering and Technology, Vol. 40, No.5, pp.397-408, 2008.

[5] Kee-Choon Kwon, et al., "Formal Verification and Validation of the Safety-critical Software in Digital Reactor Protection System," NPIC&HMIT 2006, Albuquerque, NM, USA, Nov.12-16, 2006.

[6] Sang-Hoon Lee, et al., "Validation of Reactor Core Protection System," 16th Pacific Basin Nuclear Conference, Aomori, Japan, Oct. 13-18, 2008.

[7] I. S. Oh, et al., "Development of OPERASYSTEM™ for the Non-safety I&C System Platform," ISSNP 2007, Tsuruga, Japan, July 9-11, 2007.

[8] S. M. Kwon, et al., "Development of an Advanced Power Control System for Nuclear Power Plants," ISSNP 2007, Tsuruga, Japan, July 9-11, 2007..

[9] Jung-Woon Lee, et al., "LogACTS (Logic Alarm Cause Tracking System) for a Nuclear Power Plant Operation," NPIC&HMIT 2009, Knoxville, TN, USA, April 5-9, 2009.

[10] M.S. Lee, J.H. Hong, S.H. Lee, J.K. Suh, D.H. Hwang, Development of Human Factors Validation System for the Advanced Control Room of APR1400, Journal of Nuclear Science and Technology, Vol. 46, No. 1, pp. 90-101, 2009.