GENES4/ANP2003, Sep. 15-19, 2003, Kyoto, JAPAN
Paper 1066

Advanced MMIS design characteristics of APR1400

Yeong Cheol SHIN[1], Hak Young CHUNG[2], Tae Young SONG[3]

Engineering Support Center
Nuclear Environment Technology Institute
Korea Hydro & Nuclear Power Company
103-16 Munji-dong Yusung-ku, Taejon, Korea(305-380)
Tel: [1]5770, [2]5771, [3]5774, Fax: 042-865-5704, Email: [1]ycshin, [2]hychung,[3]tysong

The basic design of Advanced Power Reactor 1400(APR1400) Man-Machine Interface System(MMIS) including control room and I&C systems has been developed to enhance the operational reliability by reducing operators' burden and to improve the cost effectiveness of plant facility by adopting integrated I&C system structure and by employing commercially available distributed control system(DCS). The APR1400 advanced control room features redundant compact workstations and a large display panel. Operator can perform, in a seated position, all plant monitoring and control tasks at any one of the workstations. The LDP provides plant level indications and alarms through which operating crew can assess plant situation including critical safety and power production functions. A safety console is provided in the main control room so that plant safety shutdown condition can be achieved and maintained through the safety console upon total failure of workstations.

Automation is done in the area of operator information processing including process representation value calculation and post accident monitoring sensor validation. Computerized procedure displays support operators in integrating procedural instructions and their associated process information to enable reliable implementation of procedures including emergency operating procedures. The NSSS/BOP control systems that have been traditionally independent, are integrated in one DCS platform and network to reduce the number of cabinets and improve the system performance and maintainability. Diversity between two groups of systems along with a few hardwired controls are reflected in the I&C architecture to cope with the common mode failure of digital plant protection system.

The APR1400 MMIS design will be first applied to the Shin-Kori 3,4 nuclear power plants, which are scheduled to go into commercial operation in 2010 and 2011, respectively.

KEYWORDS: APR1400, LDP, DIVERSITY, CMF, SOFT-CONTROLLER, I&C, MMI

I. Design concepts including control room

KNGR is, like the other advanced reactors being developed world-wide, equipped with digitialized Man-Machine Interface System(MMIS) which encompasses the Control Room Systems and Instrumentation and Control(I&C) systems, reflecting the modern computer technology. One of the main features of the I&C system is the use of microprocessor-based Multi-Loop Controllers (MLCs) for the safety and non-safety control systems. To keep the plant safety against common mode failures in software due to the use of digital systems, computers and controllers of diverse types and manufacturers will be employed in the control and protection systems. For data communication, high speed fibre optic networks are used. The remote signal multiplexer is also utilized for the safety and non-safety systems field signal transmission to save considerable amount of cables and cable trays. The I&C system will use open architecture to the extent possible for the provenness and maintainability. Since the S/W is heavily relied on in full digital MMIS, stringent S/W qualification process will be established and followed for the life cycle of KNGR. The MMIS concept to be implemented in the KNGR design is schematically depicted in Figure 1. The KNGR MCR design is characterized by 1) redundant compact workstations for CRS, RO, and TO, 2) Large Display Panel[LDP] for overall process monitoring of the plant to be shared among operating crew 3) multi-functional soft controls for discrete and modulation control, 4) Computerized Procedure System(CPS) to provide on one of the workstation CRTs with context sensitive operation guides, operational information, and navigation links to the soft controls for normal and emergency circumstances and 5) safety console for dedicated conventional miniature button type controls provided to control essential safety functions. CRT(Cathode Ray Tube)s and FPD(Flat Panel Display) are extensively used for presentation of operational information. The human factor engineering is an essential element of the control room facility design and Man-Machine Interface(MMI) design and its principles are systematically employed to ensure safe and convenient operation. Operating experience review analysis, function analysis, and task analysis are

* Corresponding author, Tel. +82-42-865-****, E-mail: ******@khnp.co.kr

performed to provide systematic input to the MMI design. Dynamic mockup has been constructed based on the simulator of predecessor plant(Korea Standard Nuclear Plant) system models. This facility was used to perform suitability analysis and V&V of the MMI design. In the forthcoming construction stage, the APR1400 specific simulator will be developed for final validation of the design.

II. Control Room Design Description

1. MCR Layout and Workstation

APR1400 MCR consists of workstations (5), safety console, large display panel(LDP) and auxiliary panels.(Refer to figure 1)[1]
The following were considered to be the key issues regarding the overall layout of the MCR:

- Visibility and size of the LDP
- Communication among operators and other control room staff
- Working area at the workstations and lay down space
- Maintainability of workstations
- Control room operation staffing in post-trip condition
- Accessibility and traffic patterns within the MCR and controlling workspace

Redundancy in the workstations is provided so that the failure of any one workstation does not prevent the operators from sharing their tasks between two operators at different workstations.
This provides a design that affords more flexibility in LDP size and location since viewing angles to the LDP are more similar for each of the two operators.

To support communication among the members in an operating crew, i.e., RO and TO, the two front workstations were located adjacent to each other.

The Shift Supervisor(SS) workstation requires similar considerations as applied to the front two workstations since it is of nearly identical design in order to serve as a backup. Additional considerations associated with the third workstation were made so that failures in a workstation would have little impact on the performance of the two operators with regard to the following:

- Communication effectiveness with the front two workstations
- Closeness to LDP for readability

One workstation is provided for Shift Technical Advisor(STA), Shift Manager(SM) and for the rest of the operating crew including local operators when it is not occupied by STA or SM. This workstation provides operational information access and workspace for the independent activities during emergency operations and this workstation may perform the backup role when one of the workstations fails. It also may serve as a supplemental work area during normal operations, minimizing intrusion of support staff into the controlling workspace.

The safety console has been located on the left side of the MCR to facilitate communication from this console with the RO and SS. These are considered to be the most likely communications that will be needed. A table is provided in the MCR for lay-down space and for team discussions among the crew. It also provides working space for the additional staff during emergency operation.

Additional space is provided in the control room for auxiliary panels such as fire protection and security.

2. Large Display Panel (LDP)

The LDP can be viewed from anywhere in the Main Control Room (MCR) and its simplicity and fixed format makes plant status easily perceived at a glance.

The choice of LDP display technology will be a project-specific selection, with its limiting size as a basic constraint dictated by the control room. Several competing technologies are presently available which potentially can support the LDP requirements.

3. Workstation Display (WSD)

Display Organization

It is not feasible to provide operator with displays for all the specific situations that can arise in a nuclear power plant. This is because all the situations and their associated knowledge for display design can not be identified because of the complex nature of a nuclear plant. Providing right set of information in a right form in a particular situation is possible in retrospect, but impossible in advance unless the plant configuration is assumed. The MMI design tailored for task only is also susceptible to the N+1 fallacy. [3]

In upper level, APR1400 WSD types are as the following;

- Large display panel(LDP) display
- Alarm display
- System display
- Critical safety function(CSF) display
- Computerized procedure(CP) display
- Global display

Multiple Display

The APR1400 workstations use multiple display devices that allow simultaneous access to a variety of plant data and information. Each compact workstation includes four FPDs for display access. Though any type of display can be assigned to any FPD, it is envisioned that any one of the FPD can be used for computerized procedures and another FPD can be used for alarm monitoring. Use of four FPDs provides adequate access to a variety of workstation

di

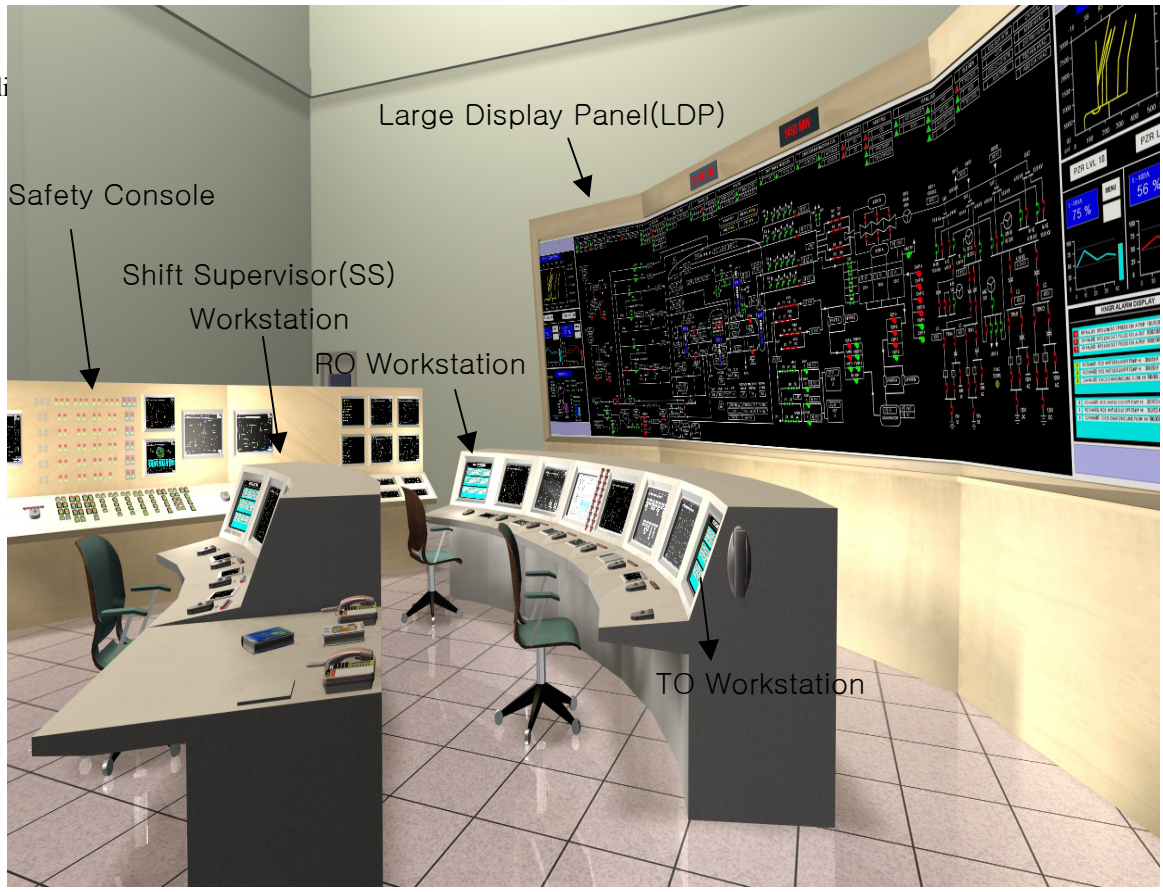

Figure 1. The Layout of APR1400 MCR

Display Access

Multiple methods are provided to allow access to the APR1400 workstation display set. The access mechanisms are designed to allow convenient and rapid access to all APR1400 workstation display pages by the operator. The following display access methodologies are incorporated;

- Navigational Access : Via this approach, logically organized display menus and display directories are utilized to allow the operator to maneuver to the desired display page(s).
- Direct Access : Via this approach, display pages may be accessed directly without the necessity of navigating through the menu or directory hierarchies.

4. Alarm System

The APR1400 alarm system is designed to improve the alarm annunciation process relative to conventional plants, by incorporating methodologies that will; [4]

- Reduce the total number of alarms that an operator must cope with
- Distinguish between a true process deviation and a sensor failure
- Minimize the occurrence of nuisance alarms
- Prioritize the relative importance of alarms so that the operator can focus on the most critical alarm condition(s) first while deferring the less critical alarm condition(s)
- Determine the impact of an alarm on plant operations and distinguish these from lower level system alarms.
- When selected in the alarm list in information FPD, RO can see only the alarms that RO has to handle while TO can see the alarms that TO has to handle.

Two separate and independent systems are utilized for APR1400 to support the alarm generation function. The QIAS processes alarm information and provides alarm annunciation at safety console. The IPS also processes alarm information and provides alarm annunciation at the workstations and the LDP. To assure consistency in alarm data between these two independent systems, the QIAS periodically sends alarm state data (as independently determined by the QIAS) to the IPS where it is compared with alarm state data as independently determined by the IPS. Any differences in alarm states between the QIAS and the IPS are annunciated by the IPS.

During the normal operation, alarm audible device located on LDP is driven by IPS. Alarm audible device on safety console is driven by QIAS only when IPS fails. The sound level of QIAS alarm is lower than that of IPS alarm.

5. Computerized Procedure System (CPS)

The APR1400 Computerized Procedure System (CPS) as shown in figure 2 is a computerized operator support system that enables an operating

crew to execute procedures with much reduced secondary tasks. It presents an overview and instructions of a procedure and related process information and controls that need to be cross-referenced to execute the procedure. The procedure information is presented on one of the four workstation information FPD. The APR1400 CPS is used in normal plant mode as well as in emergency modes. Backup paper(hard copy) procedure is used when CPS is not available. APR1400 keeps the paper procedures which licenser gives credit in current nuclear power plant. Therefore, the CPS can be treated as a supplementary operator aid. The design requires paper and computerized procedures to be subject to similar quality controls, to ensure the consistency and equivalent quality of the two systems. The design also requires paper and computerized procedures to be easily generated from the same process, to ensure consistency of the two products, and to prevent significant increase in the cost of procedure development and maintenance. [5]

CPS displays operator procedure instructions along with their associated plant process information for EOP, GOP, SOP, AOP and ARP. CPS also evaluates process conditions such as completion status of instructions, branching conditions, and re-entry condition to Continuously Applied Steps according to predefined logic. If the CPS evaluation is not consistent to operator's decision, CPS confirms if operator intends to override CPS evaluation.

The functions of CPS is shall be fully integrated with DCS, so that operator can feel that CPS display objects and pages behave in the same as any other display objects and displays in DCS. CPS shall utilize DCS MMI display objects such as parameters and components and DCS MMI display pages to the extent possible not to create a display objects twice, one for CPS and one for DCS.

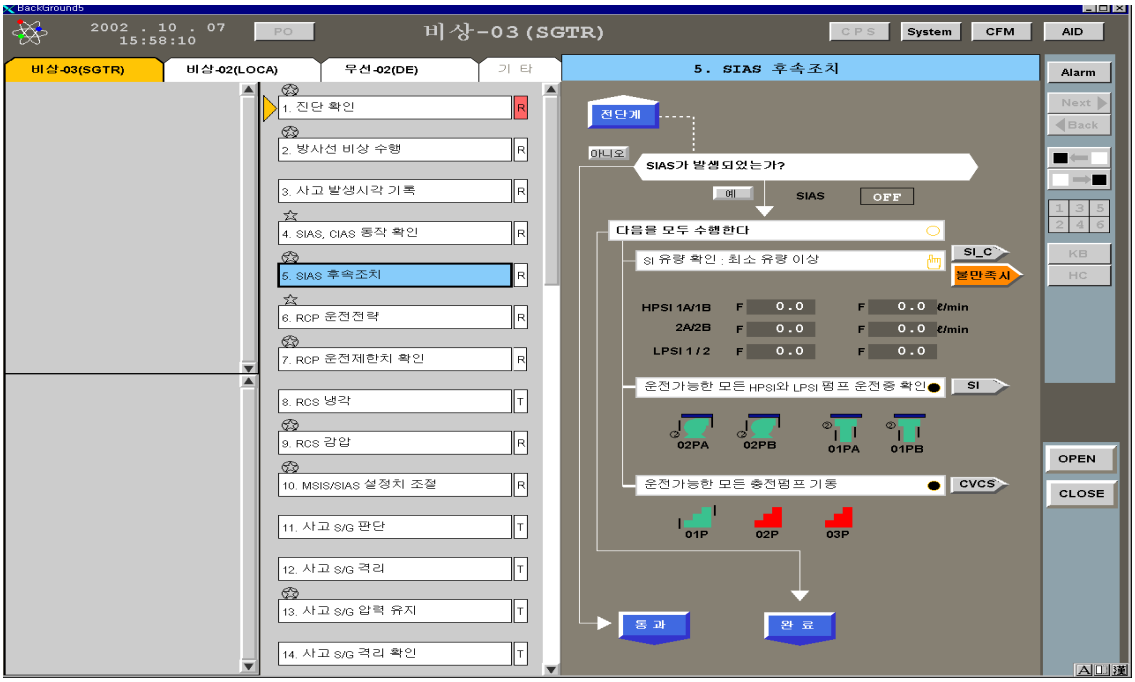

Figure 2. The Typical Computerized Procedure Display

6. Safety Console

Safety console in main control room accommodates qualified displays, qualified controls and turbine/generator backup operator interfaces, which are independent of operator interface functions of distributed control system(DCS), to support continued power operation or accident operations in case of total failure of the operator interface functions of DCS. But the safety console is also used as an operator interface station when DCS functions are normal.[1]

The safety console is intended to be used for surveillance testing during normal operations and other pre-designated operator during post-trip operation. It provides all of the required safe shutdown capabilities (including mitigation of accidents) should all of the workstation controls become unavailable due to a failure. The safety console is designed to be a sit-down and standing console.

III. I&C Design Description

1. Diversity Design

The weak point for the digital technology application is that an error-free implementation can not be achieved in adopting software into system design. So the regulatory body concern that software

design errors are a credible source of common mode failure which may defeat the safety functions in redundant, safety-related channels.

To defend against potential common mode failures (CMFs), regulatory positions as depicted in SECY-93-087 are met such that I&C D-I-D and Diversity analyses (qualitative analyses of 28 design bases events using best-estimate evaluation methodology and additional quantitative analyses using computer code for 9 design bases events) have been made in document base to show adequate diverse mitigation capability when common mode failure of protection system is assumed.

The CMF is postulated to be pre-existing when the plant disturbance occurs and to prevent both the PPS(Plant Protection System) and ESF-CCS(Engineered Safety Features Component Control System) from providing any actuation or control(automatic and manual)of their associated safety equipment. Table 1 shows that the plant functions and systems that are not affected by the CMF in the PPS and ESF-CCS and, hence, are available for the event mitigation. Operator response is necessary to help mitigate the short- term effects and to accomplish subsequent recovery actions following each event.

From this assessment, diverse means between safety and non-safety I&C systems has been applied and a set of displays (Position-4 displays) and control (Position-4 switch) located in the main control room provided for manual system level ESF actuation of critical safety functions and monitoring of parameters that support the safety function as shown in Table 2 and figure 3.

A guideline for the developing software life cycle processes for digital computer-based I&C systems which is called SPM (Soft-ware Program Manual) is developed and covered the software life cycle process planning which includes 11 documents such as software verification and validation plan and software configuration management plan etc. , the software life cycle process implementation, and the software life cycle process design output

In this SPM document, software grades applied in APR1400 I&C design are classified into 4 categories which are Safety Critical, Important to Safety (ITS), Important to Availability (ITA), and General grades.

CMFs mean in figure 3 that when there are CMFs such as software errors in PPS and ESF-CCS such that safety functions are defeated, diverse means exist in side of non-safety

Table 1. Functions assumed to be diverse and remain available after CMFs

Functions available	Related System	Operation Mode
Alternate Protection System(APS) - Reactor Trip on High Pressurizer Pressure - Reactor Trip on High Containment Pressure - Auxiliary Feed-water Actuation on Low SG Level - Manual Reactor Trip	APS	Automatic or Manual
P-CCS	P-CCS	Automatic or Manual
Manual actuation taken locally (at the component level)	-	Manual
Manual Reactor Trip	PPS	Manual
Diverse Manual ESF actuation (at a system level)	ESF-CCS	Manual
Indication, Displays and Alarms (except PPS and ESF-CCS) provided by the QIAS and IPS	QIAS IPS	-

Where
APS stands for Alternate Protection System with ITS software grade
ESF-CCS with Safety critical software grade
P-CCS stands for Process Component Control System with ITA software grade
IPS stands for Information Processing System with ITA software grade
QIAS stands for Qualified Indication and Alarm System

Table 2. Table for the I&C diversity design

Function		Diverse Means	Software Grade
Protection System	PPS	APS	ITS
	ESF-CCS	P-CCS	ITA
		Position-4 switch	Safety Critical
Monitoring System	IPS	QIAS-N QIAS-P	ITS Safety Critical

Where
QIAS-N stands for Qualified Indication and Alarm System with ITS software grade

QIAS-P stands for Qualified Indication and Alarm System for post accident monitoring and position-4 display with Safety critical software grade.

2. Characteristics of APR1400 I&C

The main control room (MCR) of the APR1400 adopts compact workstations with large display panel in front which provides key plant operating status with critical function and success path monitoring capabilities, a computerized operation procedure, and soft controller which is cooperated with IPS information and gateway database from safety and non-safety control networks and controlled by operator through FPD (Flat Panel Display) in MCB[6,7].

In accordance to this new MCR design concept, APR1400 I&C system has been designed with the network-based distributed control architecture. In this architecture, operator interface functions and control functions for NSSS, BOP and TG are integrated in common design standards and implemented in common digital system platform of DCS (Distributed Control System) except for safety system which adopts PLC (Programmable Logic Controller).

This approach makes highly functional I&C system possible with easy operation and cost-effective maintenance with the adoption of multi-loop controller. with functional segmentation for more reliable and economic aspects instead of use of several single loop controllers for one functional segment, high fidelity multiplexed fiber optic/coaxial cable data transmission for reducing cabling cost and for electric isolation, and standardized modular design with design flexibility and for easy replacement of equipment.

The plant-wide multiplexing system for both safety and non-safety systems uses high speed, fiber optic data links to significantly reduce the amount of field installed I&C cables, thereby decreasing construction time and reducing overall costs.

Universal soft controller in main control room has been applied for both safety and non-safety I&C equipment controls. A channeled CEAC (Control Element Assembly Calculator) Structure in CPCS(Core Protection Calculation System) (2-CEAC per one CPC channel) is provided, which reduces the spurious plant trip due to CEAC malfunction in existing 2-CEAC structure plant. Besides, Control functions are improved for daily load following operation with Mode-K algorithm and automatic steam generator level control at low power based on the 3-element control algorithm with steam generator level, steam flow, and feed-water flow parameters.

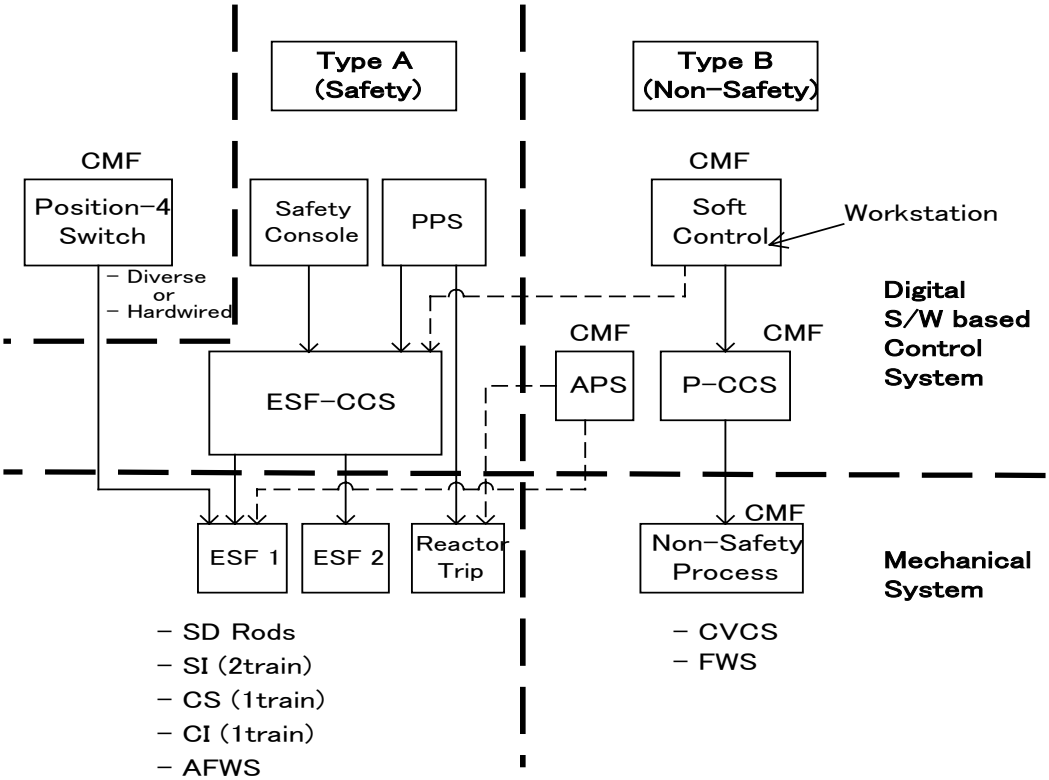

Figure 3. Diversity Design with Soft-control mechanism

Major features of APR1400 MMIS are summarized as below:

- General Features
  - Diverse Fault-tolerant Distributed Control System(DCS)

- Remote Multiplexing with Fiber Optic Communications
- Automatic Hardware Testing with Self-Diagnosis
- Common Control through Universal Soft-controller for Safety and Non-safety Systems

● Qualified Indication and Alarm System(QIAS)
- Processes Data for Alarm, Discrete Indicators, and for Process Parameters on Large Display Panel(LDP)
- Seismically Qualified

● Information Processing System
- Diverse from QIAS
- Processes Data for CRT presentation and LDP
- Implemented in the DCS data processing system
- Optical Disks for Historical Data Storage

● Plant Protection System(PPS)
- Integrated reactor Trip and Engineered Safety Feature Actuation
- Digital Core Protection Calculator (CPCs)s, Bistables and 2-out-of-4 Coincidence Logic with 2-CEAC per one CPC channel
- Initiates Reactor Power Cutback to Avert SCRAMS
- Manual Initiated Automatic Software Testing to Eliminate Most Periodic Surveillance Tests

● Engineered Safety Features-Component Control System
- Integrated Engineered Safety Feature Actuation and Emergency Load Sequencing
- Four Independent Trains

● Process-Component Control System
- Integral On/Off and Continuous
- Controls for Plant Process Systems
- Diverse from ESF-CCS

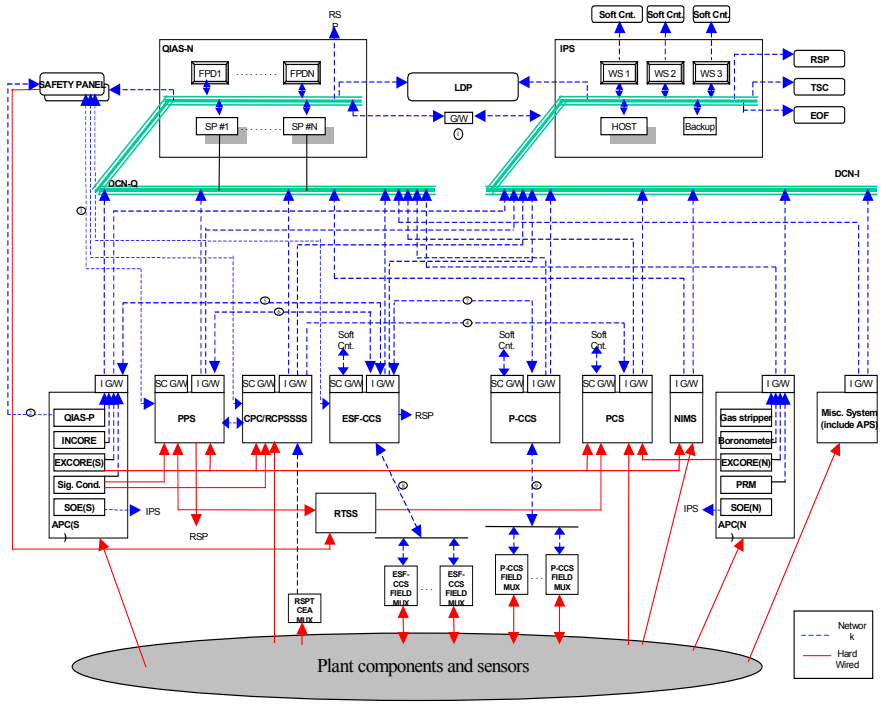

Figure 4. Overall I&C Architecture of APR1400

● Power Control System
- Daily Load Following using Mode-K algorithm
- Control Rod Position Adjusted Using Microprocessor Based Closed Loop Controllers such as Programmable Logic Controllers(PLCs) and DCS
- Reactor Regulating Controller Adjusts Reactor Power to Automatically Follow Turbine Load Changes

● Others
- Adoption of Single type Sensor of Fission Chamber for Ex-core Neutron Flux Monitoring System
- Control Signal Validation Capability

- Automatic Steam Generator Level Control over Full Power Range
- Dedicated Operator Modules with high function

The APR1400 I&C system architecture developed as shown in figure 4 which takes fault tolerant form and is composed of 4- quadrant structure i.e., safety, non-safety, and control information parts. Separation is maintained between non-safety control and information networks as much as possible but not strictly required and diversity between safety and non-safety networks. safety network meets the licensing requirements based on related criteria such as NUREG/CR-6082 "Data Communication" and NUREG-0800 SRP(Safety Review Plan)[8] for real-time performance, reliability, single-failure criterion, independence, failure mode analysis, defense-in-depth and diversity analysis, deterministic protocols, environmental qualification, and auto-testing etc.

IV. Conclusion

The design of KNGR MMIS has been completed and the detailed design is undergoing. In this paper, we discussed on the development process of the KNGR MMI, its major features, and some licensing issues for KNGR MMI. Some of the research topics to be undertaken in the future were discussed briefly as well. Presently, the licensing precedents in U.S. ALWRs provide KNGR MMI designers with general directions for addressing the issues related to full digital MMIS and human factor engineering design process of advanced control room. Systematic development of requirements and design documentation as well as early human factors evaluation of the design using a simulator-driven dynamic mockup have been achieved. This leaves the KNGR program well prepared to pursue licensing of the standard design, as well as to implement the detailed design in KNGR construction

I&C system adopts field proven off-the-shelf digital computers and networks for protective systems as well as non-safety systems, multi-loop controller with functional segmentation for more reliable and economic aspects instead of several single loop controllers for one functional segment, high fidelity multiplexed fiber optic/coaxial cable data transmission for reducing cabling cost and for electric isolation, standardized modular design with design flexibility and for easy replacement of equipment, and soft controller in main control room for both safety and non-safety I&C equipment controls.

For the resolution of license problems raised from the adoption of digital technology, I&C defense in depth and diversity analyses (qualitative analyses of 28 design bases events using best-estimate evaluation methodology and additional quantitative analyses using computer code for 9 design bases events) have been done to show adequate diverse mitigation capability when common mode failure of protection system is assumed. A guideline for the development of software life cycle processes for digital computer-based I&C systems which is called SPM (Soft-ware Program Manual) is developed.

For the functional validation for improved design features in PPS, ESFAS, CPCS, PCS, network architecture, and information systems, prototyping has been performed.

APR1400 MMIS keeps new design features of compact workstation – based MCR with large display panel, soft-controller, the adoption of field proven DCS and PLC, and system design against CMF in safety systems and so may be a leading runner which will be constructed under the recent license basis in Korea in the APWR project.

The APR1400 MMIS design will also be first applied for the Shin-Kori 3,4 nuclear power plants, which are scheduled to go into commercial operation in 2010 and 2011, respectively.

References

[1] Center for Advanced Reactor Development, KHNP, “SYSTEM DESCRIPTION for APR1400 MAIN CONTROL ROOM(Rev.A)”, 2001
[2] Center for Advanced Reactor Development, KHNP, “SYSTEM DESCRIPTION for APR1400 LARGE DISPLAY PANEL(Rev.A)”, 2001
[3] Center for Advanced Reactor Development, KHNP, “DESIGN REPORT for APR1400 DISPLAY(Rev.A)”, 2001
[4] Center for Advanced Reactor Development, KHNP, “DESIGN REPORT for APR1400 ALARM (Rev.A)”, 2001
[5] Center for Advanced Reactor Development, KHNP, “DESIGN REPORT for APR1400 COMPUTERIZED PROCEDURE SYSTEM (Rev.A)”, 2001
[6] "ALWR Evolutionary Plant Chapter 10 Man-machine Interface Systems" ALWR Utility Requirements Document Volume II ELECTRIC POWER RESEARCH INSTITUTE, Dec., 1992.
[7] "APR1400 SSAR”, Mar., 2002.
[8] "Section 7.9 Data Communication Systems" NUREG-0800 STANDARD REVIEW PLAN Nov., 1996.