# Design Feature and Prototype Testing Methodology of DHIC's Nuclear I&C System

**K.H. Kim, S.Y. Baeg, S.A. Kim, S.J. Lee, S.P. Yoon, C.Y Park**

Doosan Heavy Industries & Construction, Changwon, Republic of Korea

**Abstract.** The DHIC has developed an I&C system for a nuclear power plant through a Korean Government R&D project since 2001. This I&C system was designed and implemented to be applied for the new 1400MW nuclear power plant of KHNP. This system's design is based on the class-1E PLC platform and the non-class1E DCS platform. The PPS, the ESF-CCS, the RCOPS, the QIAS-P/N, the PCS, the NPCS, the P-CCS and the NIMS were designed, implemented and tested. The R&D project has been developed under a systematic and guided QA plan, but it is not easy to be applied for a new NPP such as Shin-Ulchin #1&2. To resolve problems of the first-application concerns, a new idea of integrated performance testing was adopted. A main control room for a verification test facility was constructed and it has features of a compact, video-based man-machine interface. The MCR includes five operation consoles, a Large Display Panel. A test system for a verification test facility is implemented as similar as a control and protection system of SUN #1&2. Integration level tests such as a system test, an interface test, a MMI test, a system function/performance test, a failure mode test, a response time test, a network load test, an alarm test, a reactor power cutback system test, an unit load transient test and a scenario test were performed using the prototype test facilities. These kinds of testing can verify and pre-validate the integrated I&C system's performance and flexibility. It could offer an implementation training before construction and also minimize trial errors to be found in the site.

## 1. KOREAN NUCLEAR I&C SYSTEM DEVELOPMENT

The DHIC(Doosan Heavy Industries & Construction) has developed an I&C(instrumentation and control) system for a nuclear power plant through a Korean Government R&D project since 2001. This I&C system was designed and implemented to be applied for the new 1400MW NPP(Nuclear Power Plants) of KHNP(Korea Hydro & Nuclear Power Co. Ltd.).

This system's design is based on the class-1E PLC(Programmable Logic Controller) platform and the non-class-1E DCS(Distributed Control System) platform. The class 1E PLC's features are a high speed processing capability, a CPU redundancy, a safety data link for communication between safety channels, a safety data network for intra channel information communication and a redundant power module. Also, the communication speed of data link and network is up to 16M bps. PLC qualification tests such as an environmental, electromagnetic interference and a seismic testing were conducted. The safety evaluation report for the PLC topical report was issued by Korean nuclear regulatory institute. The non-Class-1E DCS provides a redundant CPU/rack configuration, separated control and information networks and other necessary functions such as function blocks. The DCS's network for control and information is redundant and its communication speed is 100M bps. The speed of communication link between redundant CPU is up to 10M bps.

The PPS(Plant Protection System), the ESF-CCS(Engineered Safety Feature-Component Control System), the RCOPS (Reactor Core Protection System) and the QIAS-P(Qualified Indication and Alarming System-P) were designed, implemented and tested. The PPS has a design feature of a fault tolerant system configuration which offers the system more safety and availability. The PPS has a capability of on-line periodic logic testing. All software life cycle activities in safety system were documented and verified in conformance with the IEEE Std.1074 and the IEEE Std.1012. The safety evaluation reports for the PPS, the ESF-CCS and the RCOPS topical report were issued by Korean nuclear regulatory institute. These systems meet the Defense in depth and diversity and have simpler structures, superior abilities in maintenance and more advanced safety algorithms than previous systems used in Korea.

The PCS(Power Control System), the P-CCS(Process-Component Control System), the NPCS(NSSS Process Control System), the NIMS(NSSS Integrity Monitoring System) and the non-safety grade monitoring system were also designed, implemented and tested. The PCS has a superior ability in a DC hold power supply and a maintenance capability in power controller than previous systems used in Korea.

## 2. VERIFICATION TEST FACILITY

### *2.1. Background of Verification Test Facility Construction*

The R&D project has been developed under a systematic and guided QA(Quality Assurance) plan, but it is not easy to be applied for a new NPP such as Shin-Ulchin #1&2. To resolve problems not because of technical facts but because of the first-application concerns, a new idea of integrated performance testing was adopted. For an application of the R&D project result, the DHIC and the Korean Nuclear Utility (KHNP) organized a task-force team to evaluate and apply for the new NPP construction.

Not only for an evaluation of application to the new NPP but also for a pre-application of the developed system, an integrated verification test facility has been built. Several tests based on the KURD(Korean Utility Requirements Document) and site testing procedures are being carried. These kinds of testing can verify and pre-validate the integrated I&C system’s performance and flexibility. It could offer an implementation training before construction and also minimize trial errors to be found in the site.

Also, according to the requirements of KURD Chapter 10, the proven technology is supposed to be applied to I&C systems. Therefore, the new I&C systems should meet one of below requirements. 1) 3 years or 3, 000 Operating years as subsystem module in power plant 2) 3 years or 3, 000 operating years in other than power plant 3) prototype testing. Therefore new I&C systems are intended to meet the requirements of KURD Chapter 10 by prototype testing based on integrated verification test facility.

### *2.2. APR1400 Simulator*

The simulator developed by the KEPRI(Korea Electric Power Research Institute) for the Shin-Kori #3&4 had been used as APR1400 simulator for verification test facility. Some of the simulator codes were modified by the KEPRI, such as deletions of protection and control logics from original code for the verification test facility. The simulator developed using the WSC(Western Services Corporation)’s 3KEYMASTER™ includes a reactor thermal & hydraulic power modeling, a reactor primary system and a reactor secondary system modeling. The 3KEYMASTER™ modeling tools are a comprehensive suite of high-fidelity, efficient, object-oriented graphical modeling ones and complete with numerical solution methods. These include a flow network modeling tool, an electrical network modeling tool, a logic and control tool, a relay tool and a component library. The APR1400 reactor kinetics modeling was developed using the RELAP5-RT which is the WSC's adaptation of the Idaho National Engineering and Environmental Laboratory's RELAP5 thermal-hydraulic codes to run in the 3KEYMASTER™ environment, in real-time mode with a graphical visualization.

### *2.3. Main Control Room*

The MCR(Main Control Room) for the verification test facility uses a compact, video-based MMI(Man-Machine Interface). The MCR includes five operation consoles, a LDP(Large Display Panel). Fig.1 is the main control room’s picture of the performance test facility. The operator consoles designed to carry out plant operation by an operator include the Reactor operator(RO) console, the

Turbine Operator and the Electric Operator (TO/EO) console, the Shift Supervisor(SS) console, the Shift Technical Advisor(STA) console. Each console is composed of four control workstations and other equipment necessary for the safe and reliable operation of the plant. The LDP is installed in front of the operation consoles. It provides the capability to display plant process alarms, SGA(System Group Alarm)/Important alarms, CFM(Critical Function Monitoring) alarms, PPS status information, and plant overview status information with fixed mimic displays. The MCR also includes a Safety Console that contains Mini-LDPs and Class 1E controls for all safety-related components independent of the operator consoles. It provides the dedicated Class 1E controls for selected safety-related and non-safety components/systems and a safety related monitoring capability, including the QIAS-N/P, minimized-LDP (mini-LDP), the T/G FPD(Flat Panel Display), the ESCM(ESF-CCS Soft Control Module), the PPS/RCOPS operator module independent of the DCS operator stations and the ESCMs located at the RO, the TO, the EO, the STA and the SS Consoles.

*Fig. 1. Main control room's picture of performance test facility*

The information available to the plant operation staff both on a real-time and historical basis is processed by the IPS(Information Processing System). The major functions of the IPS include plant wide data acquisition via network, validation of sensed parameters, the execution of NSSS/BOP application programs, the monitoring of plant safety and general status, the presentation of status and calculation results on the Information displays, the provision of logs, and the determination of alarm conditions. The function of the IPS is processed by the IPS server such as a database server, an alarm server, a application server, and a historical data storage/retrieval server.

### *2.4. Test System of Verification Test Facility*

The test system for the verification test facility is implemented as similar as the control and protection system of the SUN #1&2. The test system for the PPS, the N-PCS, the NIMS and the QIAS-P/N has almost the same cabinet volume as the SUN #1&2' system. For example, the PPS is implemented as 4 channels. The other test system such as the RCOPS, the ESF-CCS, the PCS and the P-CCS has less cabinet volume than that of SUN #1&2, but the critical function representing each system was implemented. The detailed test system volume is as follows.

| Item | System Description | Prototype Volume(Cabinet) | Scope |
|---|---|---|---|
| Safety System | PPS | 12 | Fully(CH-A,BC&D) |
| | RCOPS | 4 | Partially(CH-C&D) |
| | ESF-CCS | 8 | Partially(Representative function) |

| | | | |
|---|---|---|---|
| | QIAS-P&N | 5 | fully |
| Non-Safety System | PCS | 5 | Partially (representative function) |
| | NPCS | 7 | Almost Fully |
| | P-CCS | 6 | Partially(representative function |
| | NIMS | 4 | Fully |
| MCR Equipments | LDP(Large Display Panel) | 14 | Fully |
| | Consoles(Safety Console, RO/EO/TO,SS/STA Console) | 6 | Fully |
| | Servers(Database, HDSR, Alarm, Time, Computation) | 13 | Almost Fully |

Because the test system was manufactured to interface with a plant actuation device and a sensing device directly and the APR1400 simulator is a sole computer system, an interposing system called the I/O interface panel is needed to interface the test system with the APR1400 simulator. The simulator variables for test system are implemented in I/O interface panel using National Instruments's cFP module. The simulator variables for unimplemented test system are processed by Virtual I/O.

## 3. TESTING METHODOLOGY OF VERIFICATION TEST FACILITY

The detailed test items via verification test facility are as follows:

| Test | Detailed Test Items |
|---|---|
| Electrical & Platform Function Test | Electrical Test & Redundancy Test<br>Network Communication Test<br>Controller & I/O Module Performance Test<br>PLC Function Test/DCS Function Test |
| F.A.T. | System Applications Software Module Test<br>System Test<br>Failure Mode Test/Redundancy Test |
| Integration Test (with APR1400 Plant Simulator) | Interface Test /MMI Test<br>System Function/Performance Test<br>System Response Time Test<br>Network Load Test<br>Alarm Test<br>Reactor Power Cutback System Test<br>Unit Load Transient Test/Load Cycle Test<br>Load Rejection Test<br>Scenario Test |
| Long Term Reliability (with APR1400 Plant Simulator) | Long Term Reliability Test |

### *3.1. System Test*

The purpose of the system test is to verify the basic function of the implemented system after the integration of a hardware and a software. The system test is conducted via the I/O simulator which generated simulated inputs to test system and gather output signals generated from test system. The overview of the PPS system test, as an example of system test, is as follows:

(1) Power energized status check of all modules inside cabinet.
(2) Controller booting status check via controller LED lamp.

(3) Cabinet alarm function check such as power fail detecting, low temperature alarm, cabinet door open and fan fail alarm.
(4) Bistable processor function check through simulated input signal from I/O simulator which would force bisable logic of PPS to generate bistable trip and operation bypass.
(5) Coincidence processor function check through simulated input signal from I/O simulator which would force coincident logic of PPS to generate partial trip.
(6) Operating bypass, trip channel bypass function and reactor trip and ESFAS initiation relay function test.
(7) Response time test by measuring from the time at simulated signal input from I/O simulator to the occurrence time of reactor trip.

Although detailed logic and interface signal of the other system is different from that of the PPS, the similar methods were applied to the other systems(the RCOPS, the ESF-CCS, the QIAS-P/N, the PCS, the NPCS, the P-CCS and the NIMS) for the system tests.

### *3.2. Interface Test*

The purpose of the interface test is to verify the interface function between the simulator's I/O interface panel and the individual system after the system test. The interface test is conducted via the simulator I/O interface panel which generated simulated inputs to test system and gather output signals from test system. The overview of PPS' interface test, as an example, is as follows:

(1) The signal from the simulator which would force PPS to generate reactor trip and ESFAS actuation is transferred to PPS via I/O interface panel by hardwire. For analog signal, we check if the difference, between the input value which displayed in the simulator's screen of process variable of plant and the measured value which is measured in PPS input analog module by measuring unit, dose not exceed the tolerance specified. For digital signal, we check if the simulator's signal used for operating bypass, trip channel bypass and setpoint reset logic is correctly transferred to PPS digital input module.
(2) We checked if the PPS's signal generated by logic execution, such as reactor trip and ESFAS signal, is correctly transferred to the simulator via I/O interface panel.

Although an interface signal of the other system is different from that of the PPS, similar methods were applied to the other systems(the RCOPS, the ESF-CCS, the QIAS-P/N, the PCS, the NPCS, the P-CCS and the NIMS) for the interface test.

### *3.3. MMI Test*

The purpose of the MMI test is to verify the interface and display function between the test system and the IPS. The overview of PPS' MMI test, as an example, is as follows:

(1) The PPS's signal which is generated by logic execution, such as reactor trip and ESFAS signal is transferred to IPS via channel gateway server. Channel gateway server is supplied to meet the requirement of channel isolation and electrical isolation between safety and non safety system. Channel isolation is achieved by unidirectional communication from safety system to non-safety system. We check if the PPS's signal is correctly transferred to MMI display in LDP.

Although an interface signal of the other system is different from that of the PPS, similar were applied to the other systems(the RCOPS, the ESF-CCS, the QIAS-P/N, the PCS, the NPCS, the P-CCS and the NIMS) for the MMI test.

### *3.4. System Function/Performance Test*

The purpose of system's function and performance test is to verify the function and performance of each system through the simulator. The overview of the PPS' function and performance test, as an example, is as follows:

(1) The signal from the simulator is transferred to PPS via I/O interface panel. The output signal generated by PPS logic execution, in accordance with input conditions from the simulator, is transferred to the simulator. Various PPS logics such as setpoint change logic, bistable logic, coincidence logic, operating bypass logic and trip channel bypass logic were tested.

Although detailed logic and interface signal of the other system is different from that of the PPS, the similar methods were applied to the other systems(the RCOPS, the ESF-CCS, the QIAS-P/N, the PCS, the NPCS, the P-CCS and the NIMS) for the system's function and performance test.

### *3.5. Failure Mode Test*

The purpose of failure mode test is to verify if the failure during forced simulated condition, such as a removal of card in operating normally, is detected, the symptoms due to the failure is generated in the system the same as defined in each system's failure mode effect and analysis and the system is restored after an elimination of the failure. The forced simulated condition includes the removal and the restoration of a main circuit breaker, a main power supply module, a power module of each rack, a PLC's central processing module, a PLC's communication module, a PLC input module, a PLC output module and another module in cabinet.

### *3.6. Response Time Test*

The response time test between the safety/non-safety systems and the MCR display consoles was accomplished. The response time test among the safety/non-safety systems which includes the sections between the DCS Group Controller's (NPCS) input and the DCS Loop Controller's (P-CCS) output, and between the ESF-CCS Loop Controller's input and the DCS Loop Controller's (P-CCS) output was also accomplished.

To measure the response time precisely, a dedicated measuring computer was used. The computer captures the time of the input signal from the simulator and then the time of the display output in the consoles using the USB type data acquisition device. The computer calculates the difference of times.

### *3.7. Network Load Test*

Network load data include two categories of data. One is the IPS data which is communicated between a server and a console for the periodic and the non-periodic data, and the other is the DCS data which is communicated among controllers for the control and the information data.

The basic network load data includes the data from the PPS/ESF-CCS/RCOPS/QIAS-P of the safety system, the data from the PCS/NPCS/P-CCS of the non-safety system and the data from the APR1400 simulator. These data have been already enrolled in the IPS Server as the 61,000 tags. The data flow is divided into four sections. The first is from the above systems to the server, the second is from the server to the console, the third is from the console to the FPD to display the tag data, and the last is from the console to the server to request the logging data. We have verified that the measured response time of a tag for the response time satisfied the requirement.

For the virtual network load in addition to the basic network load, the virtual controllers are set up in ten computers, and each computer generates the virtual network load of the maximum ten controllers individually. The data flow is similar to that above the basic network load test case. We have also verified that the measured response time of tag for the response time satisfied the requirement.

### *3.8. Alarm Test*

The purpose of the alarm test is to verify whether the alarm generated from the individual I&C system are displayed on the basic alarm list over the operator consoles screen through the IPS alarm server. During the alarm test, major check point is the response time between an occurrence of an alarm and an alarm generating condition, the blinking function on the basic alarm list window, the alarm sound, the alarm acknowledge function and the withdrawal of an alarm after removal of an alarm generating condition. We have also checked the alarm display functions such as the Priority Alarm / Unacknowledged Alarm / System Base Alarm / Chronological Alarm on the basic alarm list.

### *3.9. Reactor Power Cutback System Test*

The reactor power cutback system test, which is similar as the plant performance test at a plant startup stage, is to verify the functions of overall plant control systems in case 2 of 3 main feedwater pumps are failed at 70% and 95% of reactor power. The RPCS test procedures at 70% of reactor power are as follows:

(1) Two(2) main feedwater pumps are forced to trip by manual control at APR1400 simulator.
(2) It is checked if RPCS generate signals for TBN setback and TBN load increase without dropping of CEA.
(3) It is checked if TBV(Turbine Bypass Valve) is opened by SBCS(Steam Bypass Control System) automatically and MSSV(Main Steam Safety Valve) and MSADV(Main Steam Atmosphere Discharge Valve) is not opened.
(4) It is checked if setpoint of PPCS(Pressurizer Pressure Control System) and PPCS(Pressurizer Level Control System) keep up and PSV(Pressurizer Safety Valve) is not opened.
(5) It is checked if CEA is inserted by RRS(Reactor Regulation System) to regulate reactor power.
(6) It is checked if main feedwater is increased by FWCS (Feedwater Control System) and there is no initiation of RPS trip and ESF-CCS actuation.

### *3.10. Unit Load Transient Test*

The unit load transient test, which is similar as the performance test at plant start-up stage, is to verify that NSSS(Nuclear Steam Supply System) can accommodate 10% of step change from 50%, 100% reactor power and 5% per minute of a ramp change. The test procedures at 50% of a normal power are as follows:

(1) Turbine load is forced to decrease to 40% by manual control at APR1400 simulator.
(2) It is checked if CEA is inserted.
(3) It is checked if there is no initiation of RPS trip and ESF-CCS actuation and all PSVs is not opened.
(4) Turbine load is decreased to 25% as 5% per minute.
(5) Repeat step (2) and step (3).
(6) Turbine load is increased to 40% as 5% per minute.
(7) It is checked if CEA is withdrawn.
(8) Repeat step (3).
(9) Turbine load is increased to 50% from 40%.
(10) Repeat step (7) and step (8).

### *3.11. Scenario Test*

The Purpose of the scenario test is to verify the inter-system operations more clearly between the control system, the protection system and the MCR equipments, combined as a package of the individual tests. One case of various scenario tests, as an example, is as follows:

| | |
|---|---|
| Step 1: 100 % reactor power | To maintain 100% reactor power under 100% power condition of APR1400 simulator. |
| Step 2: CEA manual operation | Check if operator manually insert/withdraw CEA by Soft-control of console at 100% reactor power. |
| Step 3: Automatic load following operation (100% ->90%->100%) | Check if automatic load following operation work, while changing TBN load to 100% → 80% → 100%.<br>Check if CEA insertion status is displayed on LDP, and the parameters for PZR & SG are displayed on LDP. |
| Step 4: operation under failure of 2 out of 3 main feed-water pumps | Two main feedwater pumps are forced to trip by manual control at 100% reactor power.<br>Check if if RPCS work well and the other main feed-water pump overcome the failed condition. |
| Step 5: Reactor trip caused by PZR low pressure | To Simulate low pressure condition caused by PZR spray valve failed as stuck-opened.<br>Check if there is initiation of Reactor Protection System which generates reactor trip alarm at LDP. |
| Step 6: Check operation log | To check the time and sequence of events through Historical Data Storage & Retrieval Server(HDSR Server) during scenario test. |

## 4. CONCLUSION

The fully digitalized nuclear I&C system was developed. The Licensing (topical reports of the PLC, the PPS, the ESF-CCS and the RCOPS reviewed by KINS) was completed. The full scope of the digitalized integrated verification test facility was constructed and the verification test has been completed. We want to propose the DHIC's prototype testing methodology for a method to meet the proven technology requirement. The evaluation of the application to the SUN #1&2 project has been completed. The DHIC has closed the contract with the KHNP for the SUN #1&2 Project.

## ACKNOWLEDGEMENTS

The Nuclear I&C system development and the construction of the verification test facility was supported by Korean Government R&D programs such as the KNICS R&D program by the Ministry of Education, Science and Technology and the NUTECH-2012 R&D program by the Ministry of Knowledge Economy.

## REFERENCES

[1] Korean Utility Requirements Document, CHAPTER 10, Man-Machine Interface Systems, Korea Electric Power Corporation

[2] System Function/Performance Test Report of PPS , Doosan Heavy Industries & Construction, 2008

[3] Response Time Test Report of Verification Test Facility, Doosan Heavy Industries & Construction, 2009

[4] Network Load Test Report of Verification Test Facility, Doosan Heavy Industries & Construction, 2009

[5] Alarm Test Report of Verification Test Facility, Doosan Heavy Industries & Construction, 2009

[6] Reactor Power Cutback System Test Report of Verification Test Facility, Doosan Heavy Industries & Construction, 2009

[7] Unit Load Transient Test Report of Verification Test Facility, Doosan Heavy Industries & Construction, 2009