DEVELOPMENT AND APPLICATION OF FPGA-BASED LOGIC CONTROLLER

Yoonhee Lee, Sedo Sohn and Jaehee Yun
KEPCO Engineering & Construction Company, Inc. (KEPCO E&C)
yhlee4@kepco-enc.com; sdsohn@ kepco-enc.com; jhyun@ kepco-enc.com

Seungkweon Jeong
Woori Technology, Inc.
jeongsk@wooritg.com

ABSTRACT

The control systems of nuclear power plants contain many components which are becoming obsolete at an increasing rate. Nowadays maintenance for analog-based protection systems may be difficult as analog parts become obsolete or hard to obtain. Various studies have been conducted to address this control system hardware obsolescence issue. Those control systems of nuclear power plants have been replaced with modern digital control systems such as the programmable logic controller (PLC) and the distributed control system (DCS). The central processing unit (CPU)-based platforms such as the PLC and the DCS require an operating system (OS) and application software, and thus they might result in a common-cause failure when a problem occurs in the operating system or application software. The field programmable gate array (FPGA) is highlighted as an alternative to the conventional protection or control systems.

This paper presents the development of an FPGA-based logic controller (FLC) and a diverse protection system (DPS) with the FLC platform. Protection functions for the DPS were implemented in FPGAs without any CPU or OS.

Key Words: FPGA, FLC, DPS

1 INTRODUCTION

The CPUs of computer equipment such as PLC and DCS are difficult to qualify or certify according to the verification and validation (V&V) requirements of nuclear power plants and so they are left as black boxes. The OS of advanced computer facilities is very complex and has a lot of unnecessary features that are not needed to implement system functions for nuclear power plants.

Until now, nuclear power plants have been using FPGA only as a peripheral device of computer but recently it is expanding its application range as a main device to replace CPUs. The FPGA or the complex programmable logic device (CPLD) has been used to implement some of the board functions in PLC or to redesign the old CPU boards in Class 1E electrical circuits. In addition, attempt has been made to implement digital systems with an FPGA without using computers. The main steam and feedwater isolation system of Wolf Creek nuclear generating station in the USA was upgraded using the FPGA-based system [1]. RADIY in Ukraine has implemented FPGA-based instrumentation and control systems such as reactor trip system, engineering safety features actuation system, reactor power control and limitation system, and control rod control system for nuclear power plants [2]. Toshiba developed an FPGA-based power range neutron monitor and applied it to Kawasaki nuclear power plants [3].

Since the PLC for the DPS had been obsolete, an FPGA-based platform was considered to replace the old PLC which is diverse from the existing plant protection system. Potential manufacturers who

produce FPGA-based platforms were evaluated as hardware supplier of the DPS. Finally, it was determined to develop new FLC for the DPS.

In this paper, the FLC developed by Woori Technology in Korea is introduced in Section 2 and its application example is presented in Section 3.

2 DEVELOPMENT OF FLC

The goal of FLC development is to be as simple and optimized as possible, to eliminate the complexity of the operating system, and to meet the requirements of nuclear software development.

2.1 FLC Rack Assembly

The FLC rack assembly consists of redundant FLC modules with hot swap function, necessary input/output modules and redundant power supply modules as illustrated in Figure 1. The FLC rack assembly is fully modular with modules mounted in 19-inch chassis. It also contains a backplane that provides for distribution of power and for data signal transmission among the modules.

Figure 1. FLC rack assembly

The logic processing module (LPM) is an FLC which controls rack assembly and performs application programs. The LPM collects the data from input modules, executes a user program, and updates the data which drive the output modules. The DPS rack assembly has redundant LPMs so that the loss of any single LPM does not degrade the ability to perform user functions. In addition, the LPM includes the communication function which provides intercommunication between the FLC and an external equipment via RS-422 serial port.

The analog input module (AIM) accepts up to twenty (20) differential inputs. Analog inputs are 4-20 mA signals that vary directly as a function of the measured parameter. The AIM converts them to digital values via an analog-to-digital converter and then transmits the digitized values to the LPM. The analog output module (AOM) generates up to sixteen (16) differential outputs. Analog outputs are 4-20 mA signals that vary directly according to commands of the FLC. The AOM receives digitized values from the LPM and converts them to 4-20 mA signals via a digital-to-analog converter.

The digital input module (DIM) accepts up to 32 digital inputs (24Vdc) per module and includes input optical isolation, contact bounce filtering and front module input status indicators. The DIM reads and digitizes contact status and then transmits the digitized values to the LPM. The digital output module (DOM) has up to 24 digital outputs (24Vdc) and includes output optical isolation, short protection and front card input status indicators. The DOM receives digitized values from the LPM and converts them to contacts status.

The power supply module (PSM) provides DC power to the FLC rack assembly. The PSM is redundant so that the failure of one PSM does not impact on the operation of the DPS rack assembly.

2.2 FPGA Configuration of FLC

Reference is made to Figure 2 for FPGA configuration of the FLC. Each module has ACTEL ProASIC3 FPAGs and other necessary circuit elements without any CPU and OS.

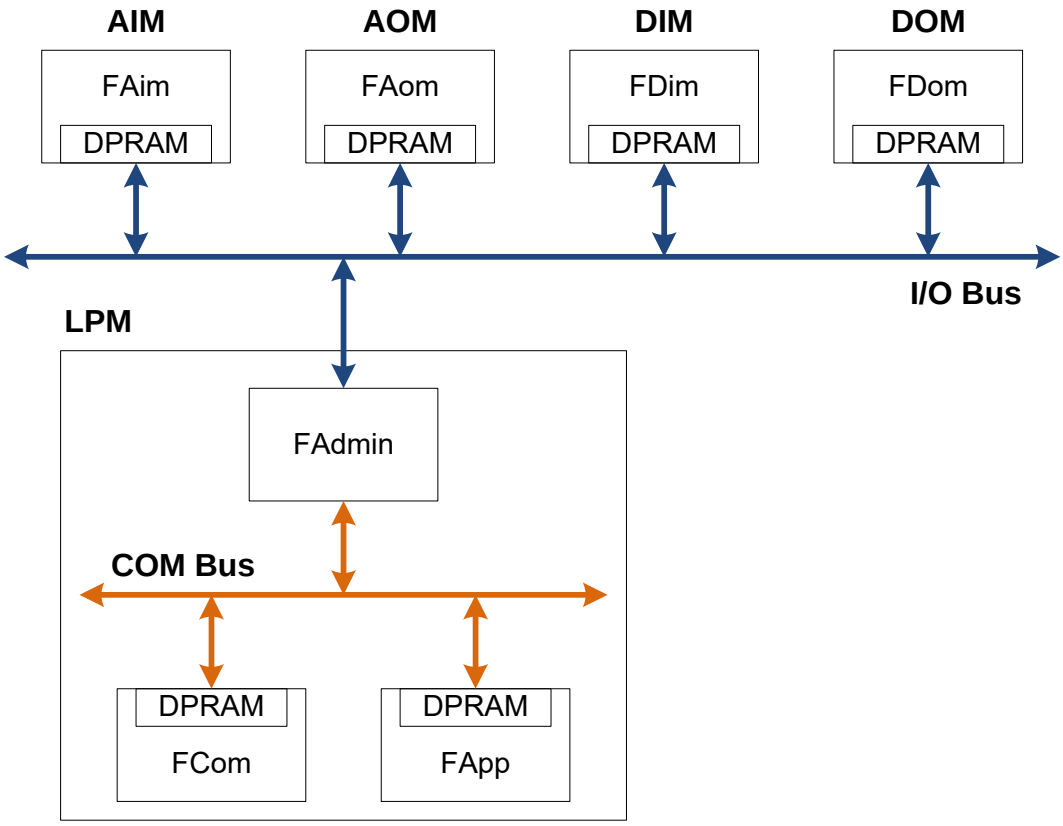

Figure 2. FPGA layout and communication flow of FLC rack assembly

The LPM has three (3) types of FPGAs: an administration FPGA (FAdmin), and a communication FPGA (FCom) and an application FPGA (FApp).

The FAdmin performs basic functions including booting, periodic execution and shutdown, data link management with input and output FPGAs, communication link management, reset, main/backup transition, and self-diagnostics of the FLC rack assembly. The FCom implements serial communications with other systems, transmitting internal information such as input/output signal values, self-diagnostics results and execution results of application FPGA, and receiving external commands. It uses parity bit, cyclic redundancy check (CRC) and sequence number to ensure the integrity of the transmitted data. User functions can be implemented in the FApp. The user program implemented in the FApp is described in Section 3.

The FLC rack assembly has input and output (I/O) bus and LPM communication bus. The I/O bus is used for data link between LPMs and I/O modules. The LPM COM bus connects three (3) FPGAs in the LPM. Parity and checksum are used to confirm the integrity of the data link between the LPM and the I/O module. In addition, the LPM and the I/O module use the heartbeat data to check the operation status.

A dual-ported random-access memory (DPRAM) technology is used to exchange data between FPGAs. The analog input module FPGA (FAim), digital input module FPGA (FDim) and FCom write their acquisition data in their own DPRAMs. The FAdmin reads the data in the DPRAMs of the FAim, FDim and FCom, writes the data in the DPRAM of the FApp, and then sends a START signal to the FApp through a separate hardwired path. When the FApp receives the START signal, it executes the user program using the data recorded in the input part of its DPRAM, records its execution results in the output part of the DPRAM, and then transmits the END signal to the FAdmin through a separate hardwired path. When the FAdmin receives the END signal, it reads the execution results of the FApp and writes them in the DPRAMs of the FAom, FDom and FCom. This operation is repeated in a deterministic manner at intervals of twenty (20) msec.

3 APPLICATION OF FLC

The goal of FLC application is to replace the old PLC-based DPS cabinet assembly while keeping the original functions. In order to apply the FLC to Hanbit Nuclear Power Plant (NPP) Units 3, 4, 5&6 and Hanul NPP Units 3, 4, 5&6, KEPCO E&C developed a new DPS cabinet assembly using the FLC in conjunction with Woori Technology. KEPCO E&C performed system design and developed the DPS application program.

Prior to the replacement of the old DPS cabinet assembly, Korea Institute of Nuclear Safety (KINS) performed the evaluation of system design using the FLC and justification on the design criteria of the DPS. As the result of its evaluation, the replacement project was approved by KINS.

3.1 Design Criteria of DPS

The DPS is intended to perform its mitigation functions in a highly reliable manner to assure the reduction of risk from the anticipated transient without scram (ATWS). The DPS is designed to provide a method of actuating reactor trip and initiating auxiliary feedwater system that is diverse from and independent of the existing reactor protection system. Summary descriptions on the design criteria for the DPS are as follows:

3.1.1 Safety class

The DPS, classified as a non-safety-related system, is not required to meet all the requirements applied to the safety systems.

3.1.2 Environmental qualification

The DPS is environmentally qualified to operate under the anticipated operational occurrences.

3.1.3 Seismic qualification

The seismic qualification is not required to the DPS, since the probability of the simultaneous occurrence of the failure of existing plant protection system and severe seismic event is too low. However, the DPS is designed to maintain the physical integrity during and after the safe shutdown earthquake (SSE) not to prevent the functions of safety system. Functional integrity is not required during the seismic event stated above.

3.1.4 EMI, RFI and surge qualification

The DPS is designed to have a sufficient quality against electromagnetic interference (EMI), radio-frequency interference (RFI), and power surge so as to perform its required functions and to ensure that safety-related instrumentation and control systems can continue to perform properly.

3.1.5 Quality assurance

The DPS is designed, procured, tested, manufactured, and handled according to NRC GL 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety-Related".

3.1.6 Redundancy

The redundancy of the DPS is not required since the existing plant protection system is already redundant. However, the DPS is designed as 2-out-of-2 channel logic to avoid malfunction due to the single failure of the system, which results in the inadvertent shutdown of the plant.

3.1.7 Manual initiation

The DPS reactor trip can be manually initiated by the operator.

3.1.8 Completion of mitigation action

The DPS is designed such that the mitigation action, once actuated, is completed.

3.1.9 Bypass

A bypass function of the DPS is provided to perform test, maintenance, repair, and calibration without actuating any inappropriate protective actions during normal operation. The bypass status is indicated in the main control room automatically and continuously. A dedicated bypass switch set is provided considering the man-machine interface (MMI).

3.1.10 Testability during power operation

A means is provided to test the DPS before installation and periodically during operation. The test for the DPS will be performed under the bypass condition, and the test from the DPS output to the final actuating devices is performed during the plant shutdown.

3.2 System Configuration of DPS

The new DPS is a two-channel non-safety related system that consists of sensors, FLC rack assembly for signal conditioning, bistable logic and coincidence logic, initiation circuit, and maintenance and test panel (MTP) for system operation. Typical cabinet configuration is shown in Figure 3.

The DPS continuously monitors pressurizer pressure, containment pressure, turbine trip status, and steam generator (SG) water levels on both channels. It automatically generates a reactor trip signal when the pressurizer pressure or the containment pressure is above its predetermined value or when the turbine trip is detected, and initiates an auxiliary feedwater actuation signal when SG water level falls below a

predetermined value. It also has a feature for manual initiation by operator's action at the main control room.

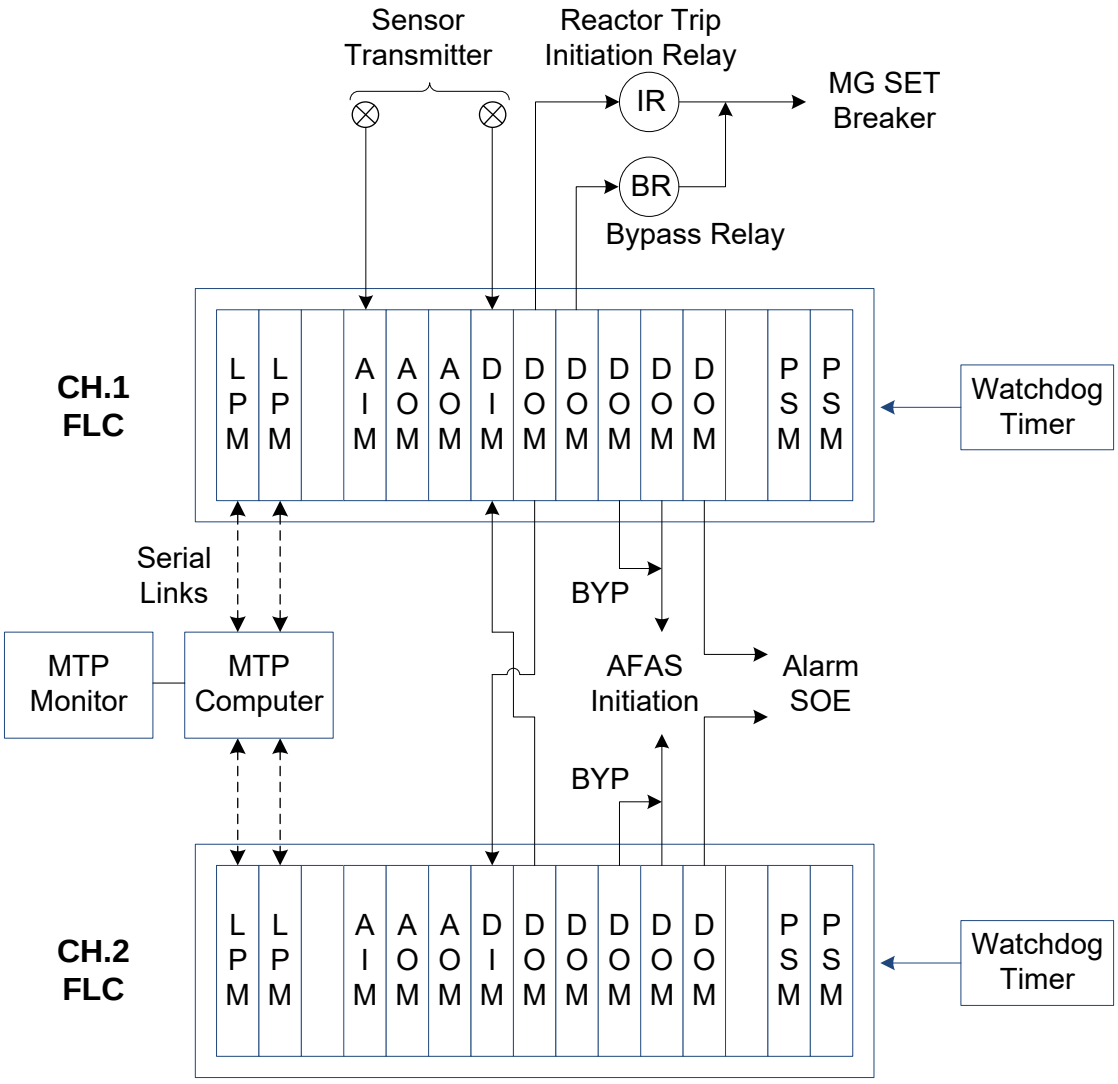

Figure 3. DPS cabinet configuration

3.3 Application Program Development for DPS

The DPS application program consists of the FPGA program for the DPS implemented in the application FPGA (FApp) and the display program implemented in the MTP.

3.3.1 FPGA program

This section introduces the development process of the FPGA program. The FPGA program is developed to meet the development life-cycle of IEC 62566 shown in Figure 4 in consideration of the specialty of FPGA programming. In addition to the verification requirements of IEC 62566, IEEE Standard 1012, which defines software V&V process, is applied to verify and validate the development

process of the FPGA program. The FPGA program is classified as the software integrity level (SIL) 3 of IEEE 1012. V&V tasks assigned to SIL 3 are performed according to the V&V plan.

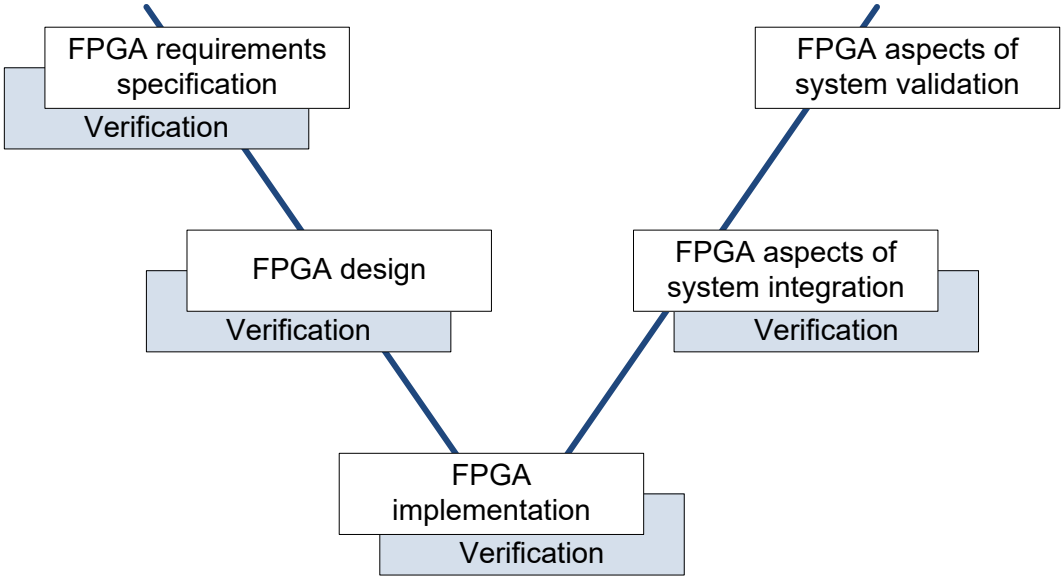

Figure 4. Development life-cycle of FPGA program

Coding standards for very high speed integrated circuit (VHSIC) hardware description language (VHDL), requirements specification, and design description for FPGA programs are produced. In the implementation stage, source files and test-bench for the FPGA program are created according to VHDL coding standards and design description. Then pre-synthesis simulation, logic synthesis, post-synthesis simulation, placement & routing (P&R), static timing analysis and post-P&R simulation are performed sequentially.

Synthesis and P&R are performed using Libero IDE v9.1 vendor development tool [4]. Functional simulation is performed to verify the DPS function using Modelsim SE simulator v10.0d [5]. The simulation is performed to satisfy 100% code coverage, and it is verified that simulation results after synthesis are the same as before synthesis, and simulation results after P&R are the same as before P&R. The Libero IDE v9.1 vendor development tool is used to measure the area occupation ratio and clock period of the FApp. Table I shows the experimental results. In Table I, the core means the basic unit of area in ACTEL FPGA. By virtue of Table I, it is confirmed that the physical requirements for FPGA are satisfied.

Table I. Experimental results

Measurement Items	Results
Occupation Ratio of Core	63.81%
Occupation Ratio of I/O	25.99%
Occupation Ratio of RAM/FIFO	12.50%
Occupation Ratio of FlashROM	100%
Clock Period	40.725MHz

Figure 5 shows the overall structure of the FPGA program for the DPS. It consists of FPGA flash ROM, bistable logic module (BLM), coincidence logic module (CLM), and channel logic control module (CLCM).

The FPGA flash ROM stores setpoint and hysteresis for pre-trip and trip of the DPS parameters. The data in the FPGA flash ROM are stored with their CRC. The BLM checks the CRC to verify the integrity of the data before using it. The setpoint and hysteresis cannot be changed through MTP, but they can be changed only through JTAG cable using the Libero IDE v9.1 vendor development tool.

The BLM includes the comparators which determine the trip and pre-trip status of DPS parameters. There is a comparator per parameter. The comparator compares converted digital value with a predefined value to determine whether or not the sensed parameter has exceeded. There are six parameters in the DPS: pressurizer pressure, containment pressure, steam generator 1 and 2 water level, turbine trip status, and manual trip status. The bistable logic for pressurizer pressure, containment pressure, and steam generator water level are based on the rising (falling) trip bistable logic with fixed setpoint. The bistable logic for turbine trip status and manual trip status is based on the binary trip bistable logic.

The CLM finally determines a reactor trip which is based on the trip status of pressurizer pressure, containment pressure, turbine trip and manual trip, and determines an auxiliary feedwater actuation which is based on the trip signals of steam generator 1 and 2 water level, using 2-out-of-2 coincidence logic between two (2) channels of the DPS.

The CLCM performs input and output functions between the FPGA program and other vendor FPGA programs and it controls the data flows for DPS functions.

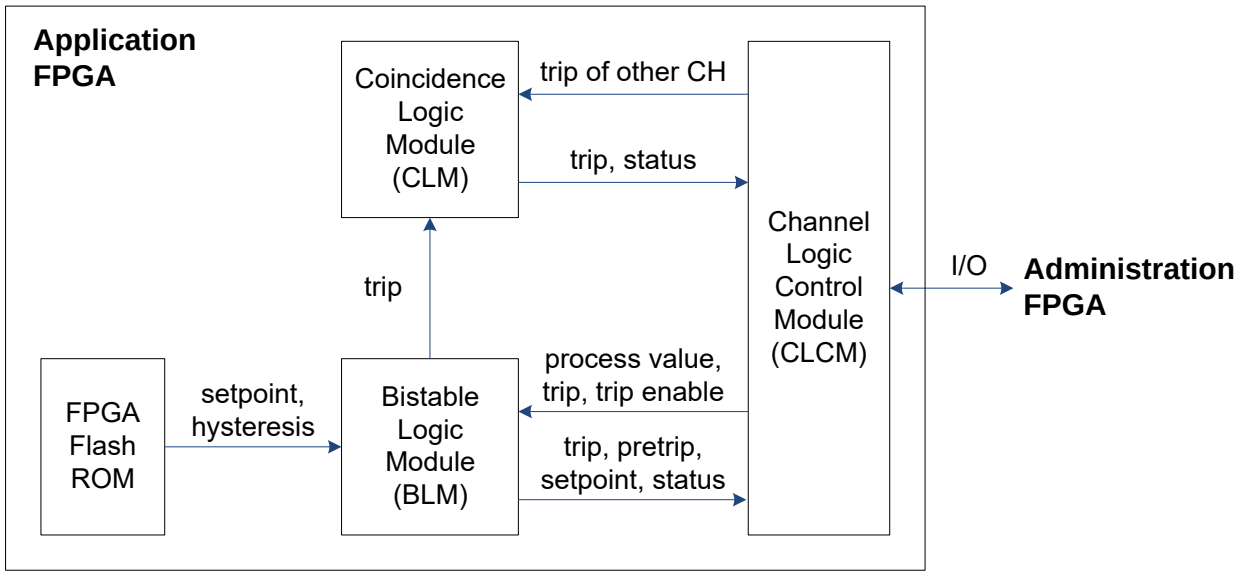

Figure 5. Overall structure of FPGA program

3.3.2 Display program

The DPS display program for the MTP is classified as the SIL 2 of IEEE 1012.

The MTP is the commercial grade computer with a flat panel display. The DPS display program, based on the QNX operating system, enables to display the data from two (2) channel FLCs.

The display program is developed using the Photon application builder which is an application programming tool of the QNX. It consists of two modules; communication and display modules. The communication module processes serial data link interface between the MTP and the FLC. It periodically receives the data from the FLC every second and updates database variables. The display module builds display pages using database information, displays them on the MTP screen and also processes operator's commands.

The MTP screen is designed to incorporate predefined human factor principles so that the displayed information can be readily perceived and comprehended by users. The human factor engineering guideline of each nuclear power plant is adopted for man-machine interface (MMI) design such as abbreviations, colors, shapes, etc. on MTP screens. The results of interview with plant operators had been reflected into the MMI design as well.

The MTP screen provides a hierarchical navigation among all hierarchical levels. The user is able to access to a display page with touch screen or mouse cursor. For example, the user can move to another display page by touching the button at the bottom of Figure 6.

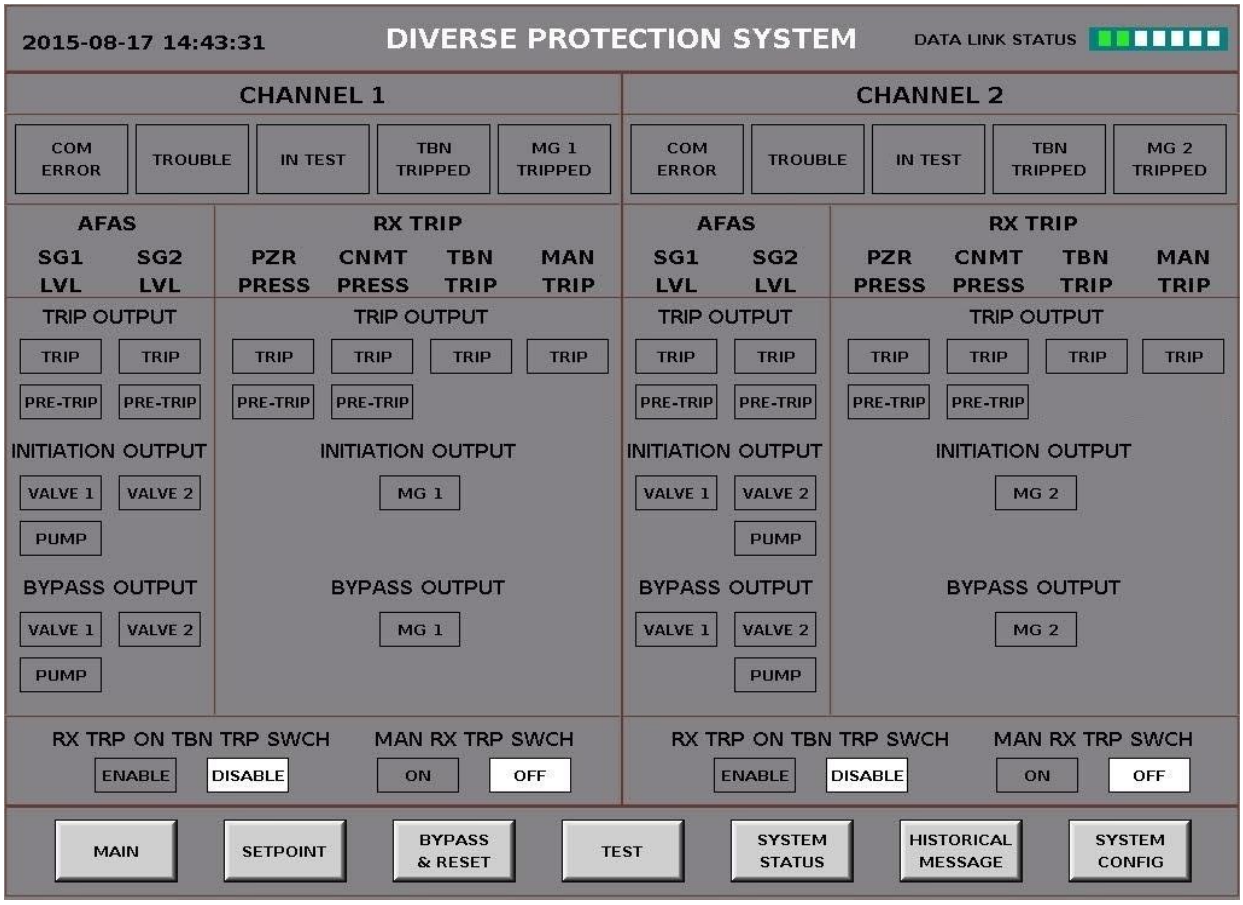

Figure 6. Main display page of MTP

The MTP screen consists of the following display pages:

1) Main display page which shows the main system operating status, pre-trip and trip status, initiation status, bypass status and main control room switch status.

2) Setpoint display page which monitors trip parameter values and setpoints.

3) Bypass and reset display page which controls the bypass of each trip function and resets the motor-generator set.

4) Test display page which initiates an automatic and/or manual test and displays the test results.

5) System status display page which shows the operating status of all modules in the FLC rack assembly.

6) Historical message display page which monitors all events that occur in the DPS.

7) System configuration display page which shows the display program version and the data link speed, and supports changing the maximum number of messages, changing the MTP password and stopping the display program.

4 CONCLUSIONS

This paper introduces the replacement of DPS cabinet assemblies at Hanbit NPP Units 3, 4, 5&6 and Hanul NPP Units 3, 4, 5&6. This paper describes design features of the FLC, design criteria and configuration of the DPS, and development of the DPS application program. Installation of the new DPS cabinet assemblies was completed in sequence with the approval of the Korean nuclear regulatory body, KINS. The operational results of the new DPS cabinet assemblies have been successful.

5 ACKNOWLEDGMENTS

We would like to thank all the project participants of Korea Hydro & Nuclear Power Co., Ltd. (KHNP), Korea Electric Power Corporation Engineering & Construction Company, Inc. (KEPCO E&C), Woori Technology, Inc. and Korea Institute of Nuclear Safety (KINS).

6 REFERENCES

1. US NRC, *Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 181 to Renewed Facility Operating License No. FPF-42 Wolf Creek Nuclear Operating Corporation Wolf Creek Generating Station Docket No. 50-482*.
2. Anton Andrashov, “Innovative Approach to Implementation of FPGA-Based NPP Instrumentation and Control Systems,” *Nuclear Safety and Simulation*, **Volume 2(4)**, pp.367-373, December 2011.
3. Toshifumi Hayashi, “Application of FPGA to Nuclear Power Plant I&C Systems,” *Nuclear Safety and Simulation*, **Volume 3(1)**, pp.51-58, March 2012.
4. Microsemi Corporation, *Actel Libero IDE User’s Guide*, v9.1.
5. Mentor Graphics Corporation, *Modelsim SE User’s Manual*, v10.0d.