Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 29-30, 2015

System and Software Design for the Man Machine Interface System for Shin-Hanul Nuclear Power Plant Units 1 and 2

Woong Seock Choi, Chang Ho Kim, Yoon Hee Lee, Se Do Sohn*, Seung Min Baek
KEPCO E&C, 989-111 Daedeokdaero, Yuseong-gu, Daejeon, 34057
**Corresponding author: sdsohn@kepco-enc.com*

1. Introduction

The Man Machine Interface System (MMIS) of the Shin-Hanul Nuclear Power Plant Units 1 and 2 (SHN 1&2) has been developed using platforms of POSAFE-Q and OPERASYSYSTEM. The design of the safety MMIS system has been performed using POSAFE-Q Programmable Logic Controller (PLC). The design of the non-safety MMIS has been performed using OPERASYSTEM Distributed Control System (DCS). This paper describes the design experiences from the design work of the MMIS using these new platforms.

2. Methods and Results

The design of the MMIS has been performed using POSAFE-Q and OPERASYSTEM. The same functions of the MMIS of the reference plants, Shin-Kori Nuclear Power Plant Units 3 and 4 (SKN 3&4) have been included. In case of SKN 3&4, the safety systems were developed based on Common Q platform supplied by Westinghouse. POSAFE-Q and Common Q platform consists of PLC type digital devices. The PLC is designed as proprietary architecture to meet its intended usage. Even the functions of the MMIS system are same as the reference plant, the architecture of the overall MMIS and each individual system have been changed to reflect the different characteristics of the platform.

The Maintenance and Test Panel and Interface and Test Processor (MTP/ITP) is included as an independent system in SKN 3&4. The MTP performs the communication path between safety systems and non-safety systems providing the communication isolation. The ITP performs the communication path among safety systems including the testing function of the Plant Protection System (PPS). In SUN 1&2, the MTP and ITP have been distributed to each system serving individual system. There are positive effects and shortcomings in this design but the implementation was affected by the platform characteristics.

2.1 PPS Design

The PPS architecture has been changed from SKN 3&4. The PPS for SHN 1&2 consists of four channels as shown in Figure 1. The PPS in each channel consists of redundant Bistable Processors (BPs) and triple redundant Coincidence Processors (CPs). The BP receives the process variables and determines the trip state by comparing the process variable values with the setpoints.

Each BP sends the partial trip status to all CPs via the Safety Data Link (SDL). The SDL is deterministic and adopts RS-485 based peer-to-peer serial communication.

The Safety Data Network (SDN) is used for communicating the status data for monitoring, alarm, testing, and etc. The SDN adopts RS-485 based bidirectional and serial network communication.

The CP determines the state of the coincidence output based on the status of the four pairs of trip inputs. Each reactor trip initiation outputs are combined in a 2-out-of-3 coincidence in the initiation circuit as shown in Figure 1. The redundancy in each channel increases the availability and operability.

The SHN 1&2 PPS was developed to have the redundancy in each channel and to use the benefits of POSAFE-Q PLC, such as diagnostic and data communication. In addition, the manually initiated automatic logic testing functions are provided for the PPS to reduce the operator burden.

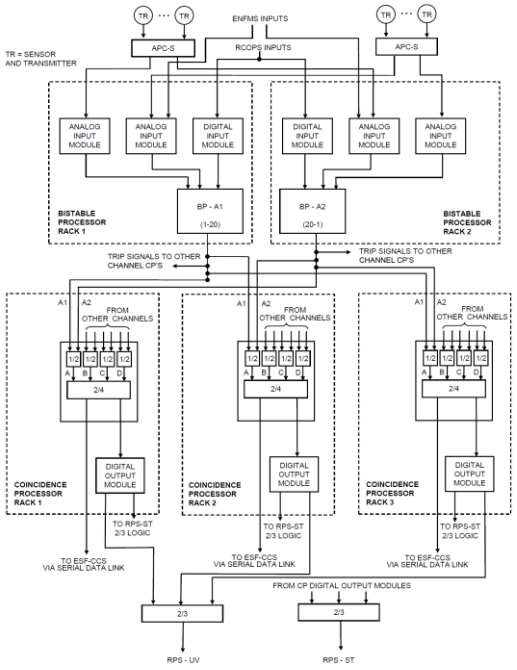

Fig. 1. PPS Configuration (Channel A)

2.2 RCOPS Design

The Reactor Core Protection System (RCOPS) has been redesigned to reflect the operating experience and platform characteristics. In case of SKN 3&4, two CEAC (Control Element Assembly Calculators) per channel were installed to meet the original system. But in SHN 1 and 2, only one CEAP (Control Element Assembly Processor) per channel has been installed to utilize data sharing as shown in Figure 2.

Two (2) separated reed switches are installed for one CEA housing in the standard PWR (Pressurized Water Reactor). Each Core Protection Processor (COPP) of a channel 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 which are used to calculate Local Power Density (LPD) and Departure from Nucleate Boiling Ration (DNBR).

The CEA Processor (CEAP) takes all CEA positions of the reactor core through Channel Communication Processor (CCP) and examines the CEA deviation based on subgroup. If this deviation is higher than a specified value the CEAP sends the penalty factor to the COPP.

The Reed Switch Position Transmitter (RSPT) signals representing CEA positions are acquired by the CCP analog input cards. There are two separated RSPTs called RSPT1 and RSPT2. RSPT1A ("A" section of RSPT1) signals are measured by channel A CCPs. RSPT1B, 1C and 1D signals are measured by channel B CCPs. RSPT2D ("D" section of RSPT2) signals are measured by channel D CCPs. RSPT2A, 2B and 2C signals are measured by channel C CCPs. Channel A CCPs and channel B CCPs exchange their RSPT1 signals to build whole area of CEA position of RSPT1. Channel C CCPs and channel D CCPs exchange their RSPT2 signals to build whole area of CEA position of RSPT2.

Two CCPs are installed on each channel for redundancy. The COPP takes RSPT signals of the corresponding quadrant of the reactor core called target CEA position through CCP. The COPP takes the penalty factors from 4 CEAPs of all channels and selects the largest value for conservativeness and uses it to calculate the DNBR and LPD.

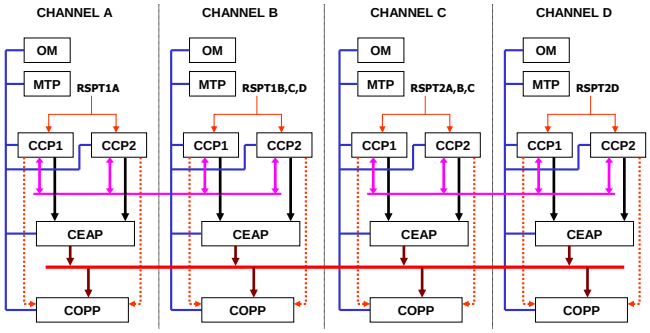

Fig. 2 Block diagram of RCOPS

2.3 DPS Design

The design of the non-safety system has been performed using OPERASYSTEM. In case of SKN 3&4, the platform for the non-safety systems is based on OVATION which was supplied by Westinghouse. The Diverse Protection System (DPS) design has been changed from SKN 3&4 to incorporate platform characteristics and to reinforce cyber security. The DPS controllers for SKN 3&4 are directly connected to the OVATION network and identified as nodes of the DCS. The connection of the DPS and other non-safety systems, in particular Microsoft Windows based operator workstations via DCS networks may incur a risk. There might be potential for disturbances of the DPS function due to malfunction of the non-safety system. Failures may propagate spreading wrong data although the probability is very low.

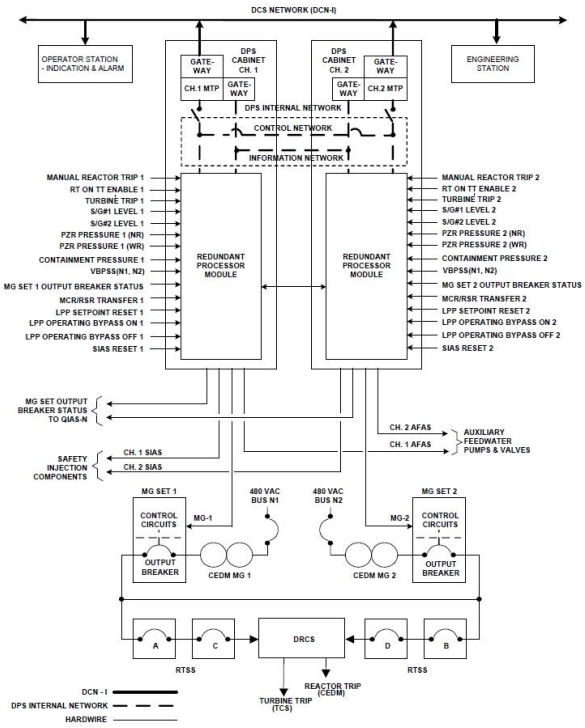

Fig. 3. DPS Configuration for SHN 1&2

Figure 3 shows the SHN 1&2 DPS MTPs are directly connected to the OPERASYSTEM network. The DPS MTP is identified as a node of the DCS but the DPS controllers are not. The DPS MTP only provides unidirectional communication to other non-safety systems and so the DPS controllers are fully separated from the DCS network.

2.4 Application Software Development using Commercial CASE Tool

The safety-critical software has been developed under the environment that requires a lot of effort, cost, and time in documentation oriented manner. In SHN 1&2, certified CASE (Computer Aided Software Engineering) tool has been used for effective software development of the PPS and QIAS-P. With CASE tools, the development efforts and human errors can be reduced and software quality can be improved, productivity, and reusability. KEPCO E&C has setup the development environment, named the Integrated Software Development Environment (ISODE), which is composed of a set of tools and procedures dedicated to the safety-critical software development. The whole processes for software development work are presented in Figure 4.

Modeling, Debugging, and Simulation were performed by software development engineers using SCADE. The Requirement Traceability Matrix (RTM) was produced using DOORS Tool which is the requirements traceability tool. Code review and module test were performed after code programming using pSET which is target design tool.

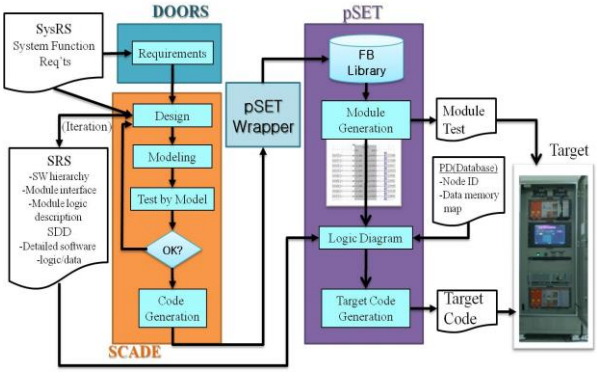

Fig. 4. PPS S/W Development Process

3. Conclusions

The SHN 1&2 MMIS has been developed using POSAFE-Q platform for safety and OPERASYSTEM for non-safety system. Through the utilization of the standardized platform, the safety system was developed using the above hardware and software blocks resulting in efficient safety system development. An integrated CASE tool has been setup for reliable software development. The integrated development environment has been setup formally resulting in consistent work. Even we have setup integrated development environment, the independent verification and validation including testing environment needs to be setup for more advanced environment which will be used for future plant.

REFERENCES

N/A