System and Software Design for the Plant Protection System for Shin-Hanul Nuclear Power Plant Units 1 and 2

In Seok Hwang*, Young Geul Kim, Woong Seock Choi, Se Do Sohn
KEPCO E&C, 989-111 Daedeokdaero, Yuseong-gu, Daejeon, 34057
**Corresponding author: narosoo@kepco-enc.com*

1. Introduction

The Plant Protection System (PPS) performs Reactor Protection System (RPS) functions and Engineered Safety Features Actuation System (ESFAS) functions. The RPS protects the core fuel design limits and reactor coolant system pressure boundary for Anticipated Operational Occurrences (AOOs), and provides assistance in mitigating the consequences of Postulated Accidents (PAs). The ESFAS sends the initiation signals to Engineered Safety Feature – Component Control System (ESF-CCS) to mitigate consequences of design basis events.

The Common Q platform Programmable Logic Controller (PLC) was used for Shin-Wolsung Nuclear Power Plant Units 1 and 2 and Shin-Kori Nuclear Power Plant Units 1, 2, 3 and 4 since Digital Plant Protection System (DPPS) based on Common Q PLC was applied for Ulchin Nuclear Power Plant Units 5 and 6. The PPS for Shin-Hanul Nuclear Power Plant Units 1 and 2 (SHN 1&2) was developed using POSAFE-Q PLC for the first time for the PPS. The SHN1&2 PPS was delivered to the sites after completion of Man Machine Interface System Integrated System Test (MMIS-IST).

2. Methods and Results

The SHN1&2 PPS has the design features as follows:

2.1 Configuration

The PPS consists of four channels and meets the single-failure criterion in Reference 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. 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.

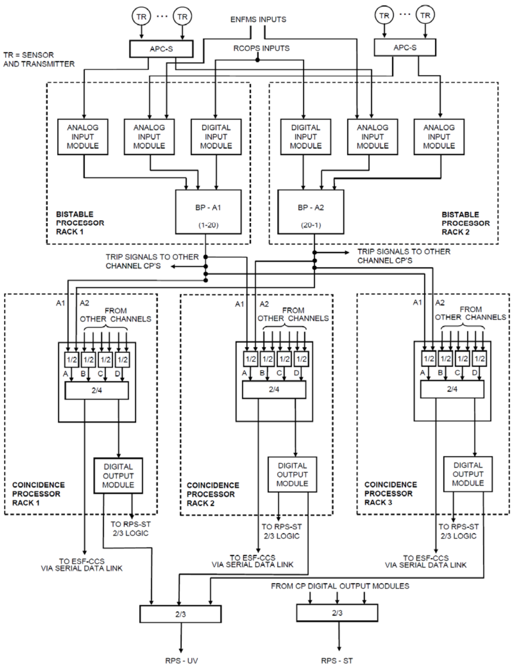
TR
TR
ENFMS INPUTS
TR
TR
APC-S
RCOPS INPUTS
APC-S
TR = SENSOR AND TRANSMITTER
ANALOG INPUT MODULE
ANALOG INPUT MODULE
DIGITAL INPUT MODULE
DIGITAL INPUT MODULE
ANALOG INPUT MODULE
ANALOG INPUT MODULE
BP - A1 (1-20)
BP - A2 (20-1)
BISTABLE PROCESSOR RACK 1
BISTABLE PROCESSOR RACK 2
TRIP SIGNALS TO OTHER CHANNEL CP'S
TRIP SIGNALS TO OTHER CHANNEL CP'S
A1
A2
FROM OTHER CHANNELS
1/2
A
B
C
D
2/4
DIGITAL OUTPUT MODULE
COINCIDENCE PROCESSOR RACK 1
COINCIDENCE PROCESSOR RACK 2
COINCIDENCE PROCESSOR RACK 3
TO RPS-ST 2/3 LOGIC
TO ESF-CCS VIA SERIAL DATA LINK
FROM CP DIGITAL OUTPUT MODULES
2/3
2/3
RPS - UV
RPS - ST

Fig. 1. PPS Configuration (Channel A)

2.2 Signal Quality Checking Logic

The PPS which includes Signal Quality Checking Logic (SQCL) meets fault detection and self-diagnostics requirements in Reference 2. All signals within the PPS have the quality attribute which is specified as “Good” or “Bad”. Downstream signal processing algorithm detects the faults resulting from processor and communication failures to determine the signal quality. The SQCL in the BP and the CP reads the results of the diagnostic task from assigned registers. Diagnostic task periodically checks the integrity of hardware and software. The BP sends the signal quality to the CP. The CP determines the quality attribute of the signal based on the signal quality received from the BP and the diagnostic results associated with the signal path including the communication. The quality attribute is used in application program as shown in Figure 2.

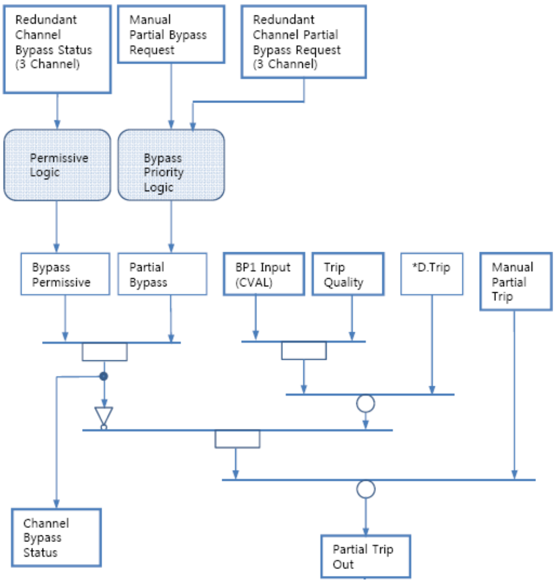

Fig. 2. CP Partial Trip Processing Logic

2.3 CP Processing for Redundant BP signals

When the quality of the signal from one BP is "Bad", data from the other BP in the affected channel is used in all CPs. In the event that both bistable partial trip data from one channel are indicating bad quality, the channel is set to the trip condition for reactor trip functions. In the event that both bistable partial trip data from one channel are indicating bad quality, the channel is set to the non-actuate condition for ESFAS functions. The ESFAS functions are treated differently when the both BPs fail because of the adverse consequences of an inadvertent ESF actuation.

2.4 Channel Functional Test

The PPS Automatic Test covers the hardware tests from Analog Input Module to the contacts of initiation circuits for the RPS function and to the output of initiation logic in the CP for the ESFAS function as well as software logic tests in the BP and the CP. The majority of Surveillance Requirements in Technical Specification can be met by PPS Automatic Test as shown in Figure 3. Manual Test will be performed for the parts which were not covered by Automatic Test. The Surveillance Test applying Automatic Logic Test will minimize the operator burden and reduce testing time because Automatic Logic Test does not require frequent manual actions. The PPS meets the surveillance testing requirements in Reference 3.

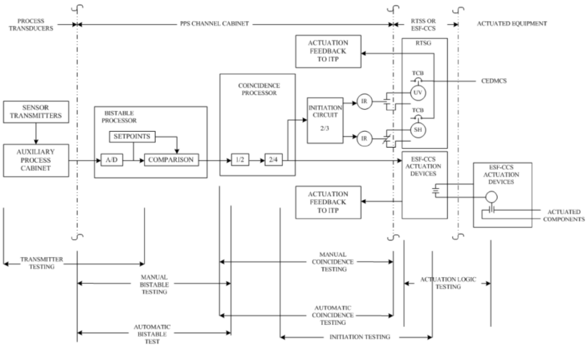

Fig. 3. PPS Testing Overlap

2.5 Data Communication

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. Each SDL communication memory block consists of sending area and receiving area, each with 512 words. Separate communication memory blocks are assigned to prevent overlap between incoming data and outgoing data.

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 SDN communication sends and receives data based on index unit. Each index consists of sending area and receiving area, each with 110 words. Separate indexes are assigned to prevent overlap between incoming data and outgoing data. Data communication for the PPS was designed to meet the communication independence requirements in Reference 2.

2.6 PPS Application Software Development using Commercial CASE Tool

The safety-critical software has been maintaining a manpower-based development system that traditionally requires much effort, cost, and time in accordance with regulatory guides, especially focused more on producing, verifying and validating various documents than software development itself.

Consequently, the need is on the rise for a certified tool such as the CASE (Computer Aided Software Engineering) tool for effective software development upon full digitalization of instrumentation and control system in nuclear power plants. Commercial tools are needed for systematic approach in software development, reducing development time and human errors, and improving software quality, productivity, and reusability. Based on the qualitative and quantitative evaluations, the SCADE tool from Esterel Technologies was selected as the CASE tool for software development for the PPS.

KEPCO E&C has been developing the software development environment, named the Integrated Software Development Environment (ISODE), which is composed of a set of tools and procedures dedicated to safety-critical software development. The whole processes for software development work are presented in Figure 4.

The documents generated using ISODE are Software Requirement Specification and Software Design Description.

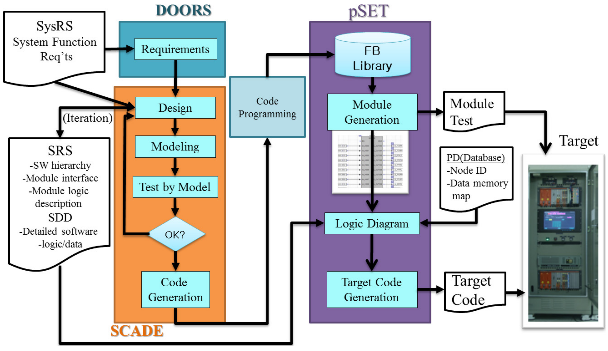

Fig. 4. PPS S/W Development Process

Modeling, Debugging, and Simulation were performed by software development engineers using SCADE. The Requirement Traceability Matrix (RTM) was performed using DOORS Tool. Code review and module test were performed after code programming using pSET.

KEPCO E&C developed safety-critical software for BPs and CPs of the PPS for SHN 1,2 using ISODE.

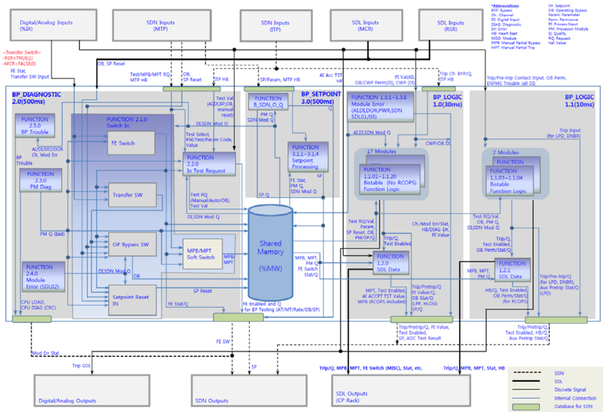

Fig. 5. Module Design for the Bistable Logic Software

The module structure of the BP software is shown in Figure 5. The bistable logic consists of BP_LOGIC which processes bistable function, BP_SETPOINT which processes the setpoint data, and BP_DIAGNOSTIC which processes diagnostic function and test function. The BP consists of 19 bistable variables and each variable is implemented with several modules in ISODE. Within each module, the sub-modules that perform the functions described above are included.

The module structure of the CP software is shown in Figure 6. The coincidence logic consists of the CP_LOGIC which processes coincidence function and CP_SUPERVISING which processes diagnostic function and test function.

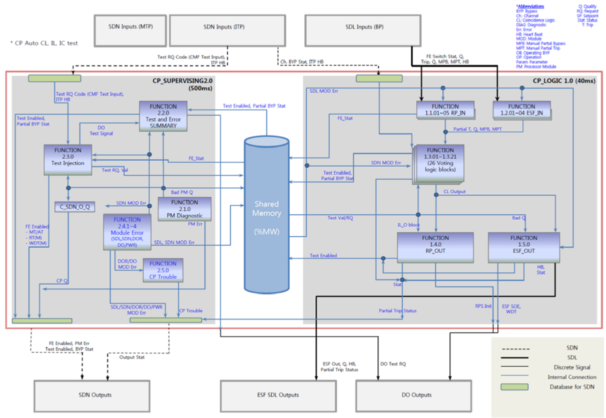

Fig. 6. Module Design for the Coincidence Logic Software

3. Conclusions

The SHN1&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 lower the operator burden. The PPS application software was developed using ISODE to minimize development time and human errors, and to improve software quality, productivity, and reusability.

REFERENCES

[1] IEEE 603-1998, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”.
[2] IEEE 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations”.
[3] IEEE 338-1987, “IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems”.