PPS Design and Software Testing for SHN 1 & 2

Sedo Sohn , YoungGeul Kim, WoongSeock Choi, ChangJae Lee*
KEPCO Engineering & Construction Company Inc., 150-1 Deokjin-Dong, Yuseong-Gu, Daejeon, Korea, 34057
**Author: cjlee1@kepco-enc.com*

1. Introduction

The Plant Protection System (PPS) has been developed using qualified Programmable Logic Controller (PLC) for safety application. The PPS monitors the plant process variables, generates signals to trip the reactor and actuate the engineered safety features. The PPS is configured in 4 redundant channels to meet single failure criteria, capability for testing and calibration, and high reliability. The PPS is implemented considering the proprietary PLC architecture and data communication characteristics. The PPS has been developed to achieve high reliability with minimum inadvertent actuation of the safety functions. The PPS software has been developed to meet the related regulatory guidelines and standards such as IEEE 7-4.3.2 [1] and IEEE 1012 [2]. For the PPS software development, CASE (Computer Aided Software Engineering) tools have been used for effective software development. PPS software V&V (Verification and Validation) has been performed extensively to verify its correctness and completeness.

2. PPS System and Software

Plant Protection System (PPS) monitors the plant process variables and generates reactor trip signals and engineered-safety features (ESF) actuation signals to protect the plant from accidents. PPS monitors the reactor power level, steam generator pressure, steam generator level, pressurizer pressure and level, reactor coolant flow rate. If the measured process variables exceed the trip setpoint the trip or ESF actuation signals are generated.

2.1 PPS Implementation

The PPS is configured in four channels to meet the single failure criteria and to allow channel bypass during maintenance testing. Each channel of the PPS consists of Bistable logic processor (BP), local coincidence logic processor (CP), interface and test processor (ITP), maintenance and test processor (MTP), and operator module (OM). The BP reads the process signals and compares the signals against its setpoint and generates the digital outputs. The plant process input signals to PPS such as Pressurizer pressure, and neutron flux signals are selected during safety analysis. The CP reads the outputs of BP processors and performs two-out-of-four voting logic to generate the reactor trip or ESF actuation signals. The MTP is provided for periodic surveillance testing of the system to check the functionality of the system. OM receives the data from BP and CP over the communication network to display the system status and actuation output status.

The PPS is designed using nuclear qualified class 1E PLC hardware. The PLC includes processor module, analog input module, digital input module, digital output module, and communication modules. The processor module reads the analog or digital inputs and performs the logic and generates the output signals through digital output module. When reading the analog input signals, the diagnostic signals are also provided to the processor module such that the processor module monitors the validity of the input signal for the signal range and input module health. The processor module reads the input signal through the serial communications and the integrity of the data communication is always checked when reading the input signal.
The protection logic checks the validity of the input signal every time the signals are used. If the signal validity is bad, then the signal condition is alarmed to the operator and redundant signal is used if there is a redundancy.
Even though PLC is widely used in the safety system design, each PLC has unique design characteristics depending on the manufacturer. The design of the system using the PLC is affected by the architectural and functional characteristics of the PLC processor.
There are redundant BPs (Bistable Processors) in each channel. Each BP receives its input signal from associated input channels and performs comparison logic to generate output signals. The outputs of BPs are communicated to the other channels via Safety Data Link. These two BP outputs transmitted to CPs go through OR logic before they are used as input to CPs. These CPs in each channel performs 2-out-of-4 voting logic. The outputs from CPs actuate contact outputs to actuate trip breaker of the Reactor Trip Switch Gear. In addition, the outputs of CPs are sent to ESF component control system (ESF-CCS) to actuate ESF components.

2.2 PPS Software Design

The safety-critical software has been developed by documentation oriented waterfall model. In SHN (Shin Hanul Nuclear Power Plants) 1&2, certified CASE tool has been used for effective software development of the PPS. With CASE tools, the development efforts and human errors can be reduced and software quality can be improved, along with

productivity and reusability. KEPCO E&C has set up the development environment composed of a set of tools and procedures dedicated to the safety-critical software development.

2.3 PPS Software V&V

The software Verification and Validation (V&V) has been performed to meet the regulatory requirements and standards such as IEEE 1012 [2]. The software is classified into four different classes based on the criticality of the software assigned for the system. PPS PLC software performing safety function is classified as safety critical class which corresponds to SIL 4 in IEEE 1012 [2]. For safety critical software, the V&V process should be accompanied with the thorough review process and testing at each development phase. The verification and validation is performed by independent engineering group. During development process, the V&V group performs document verification, requirement traceability analysis, and code review. After completion of software implementation by design group, the software is turned over to the V&V group through software configuration control tool.

The PPS software is tested to meet the IEEE 1012. The component testing is performed for every module to meet the branch coverage. The test cases are generated using test tool to confirm the branch coverage of 100%. Then the module is loaded into the PPS test hardware to confirm that the execution results are correct during Module Testing(MT). Then the testing is performed on a unit program basis. Unit Testing(UT) is executed as a separate task in the processor. Every functional requirement in the software requirements specification is executed in the unit testing. Then the integrated testing is performed in the software and hardware combined environment during One Channel Software Testing(OCST). The hardware anomaly such as input signal out of range, input card fault conditions are executed. Processor overload conditions are executed and CPU overloading conditions are detected. Also the man machine interface of the display output is tested for correct display.

The PPS software were released for verification and validation testing with BP, CP software at Oct. 2011 and ITP, OM/MTP software at July 2012. V&V team performed testing of the PPS after software release. The exceptions found during testing are recorded and transmitted to the design group as TERs (Test Exception Report), and design group provides resolution for the exceptions and write SCRs and implements the changes. After completion of changes, the software is released to the V&V group and regression testing is performed.

The findings were mostly found in two years after initial release. There were 103 TERs in 2012, 120 TERs in 2013, 1 TERs each in 2016, 2017, and 2 TERs in 2018. Module testing resulted in 14 TERs, Unit testing resulted in 93 TERs, One Channel Software Test resulted in 110 TERs. These results show that the finding were more related to the hardware-software interfaces and man machine interfaces. SCRs are issued for each TERs issued by V&V team to correct the findings, but many were issued by software design team themselves. The design team revised software to implement hardware manufacturer and user's request in addition to anomaly in TERs. To implement these changes, SCRs (Software

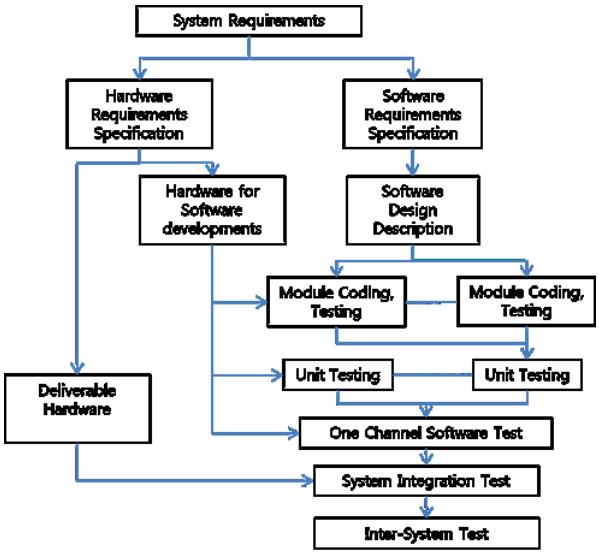

Figure 1 Software Testing Scheme

Change Request) were issued. There have been 182 SCRs in 2012 issued including 4 SCRs issued in 2011, 240 SCRs in 2013, 32 SCRs in 2014, 13 SCRs in 2015, 19 SCRs in 2016, 16 SCRs in 2017, 23 SCRs in 2018, 12 SCRs in 2019.

The changes include errors in variable connection, memory assignments, and test logic, etc. The errors found during module testing were mostly implementation errors of coding. The errors found during unit testing include test procedure errors. Most of the errors found during OCST are related to the diagnostic related errors and display related errors. Display errors were human interface related errors such as use of inconsistent variables, inconsistent status display, and incorrect alarm etc. Diagnostics errors were related to trouble alarm consistency, equipment diagnostics, incomplete test logic, and signal quality etc.

3. Conclusions

Many of the display and diagnostics related software errors were detected during the test phase, and revisions of software by user's request such as display consistency among systems have occurred since software release to the user. One of the disadvantage of the waterfall model life cycle is clearly shown in the number of corrections that has occurred. Even after the software development has been finished, more efforts have been required to improve MMI aspect of the system display. So it might be better to adopt rapid prototype model for the display

software and introduce human factor engineering verification and validation in parallel.

REFERENCES

[1] IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2003
[2] IEEE Standard for Software Verification and Validation, 2004