PPS Design and Software Testing for SHN 1 & 2

KEPCO E&C

Sedo Sohn , YoungGeul Kim, WoongSeock Choi, ChangJae Lee*

I. Introduction

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

2.1 PPS Implementation (1/3)

- PPS is configured in four channels to meet the single failure criteria and to allow channel bypass during maintenance testing.
  - 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).
  - BP reads the process signals and compares the signals against its setpoint and generates the digital outputs.
  - CP reads the outputs of BP processors and performs two-out-of-four voting logic to generate the reactor trip or ESF actuation signals.
  - 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.

2.1 PPS Implementation (2/3)

- PPS is designed using nuclear qualified class 1E PLC hardware.
  - PLC includes processor module, analog input module, digital input module, digital output module, and communication modules.
  - When reading the analog input signals, the diagnostic signals are also provided to the processor module for validity of signal range and input module health.
  - When processor module reads the input signal through the serial communications, the integrity of the data communication is always checked.
  - protection logic checks the validity of the input signals 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.

2.1 PPS Implementation (3/3)

- PPS architecture is affected by characteristics of the PLC
- 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.
  - two BP outputs transmitted to CPs go through OR logic before they are used as input to CPs.
  - The outputs of BPs are communicated to the other channel CPs via Safety Data Link.
- CPs in each channel performs 2-out-of-4 voting logic.
  - outputs from CPs actuate contact outputs to actuate trip breaker of the Reactor Trip Switch Gear.
  - outputs of CPs are sent to ESF component control system (ESF-CCS) to actuate ESF components.

2.2 PPS Software Design

- The PPS software has been developed based on waterfall model life cycle with documentation-oriented manner.
- 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.

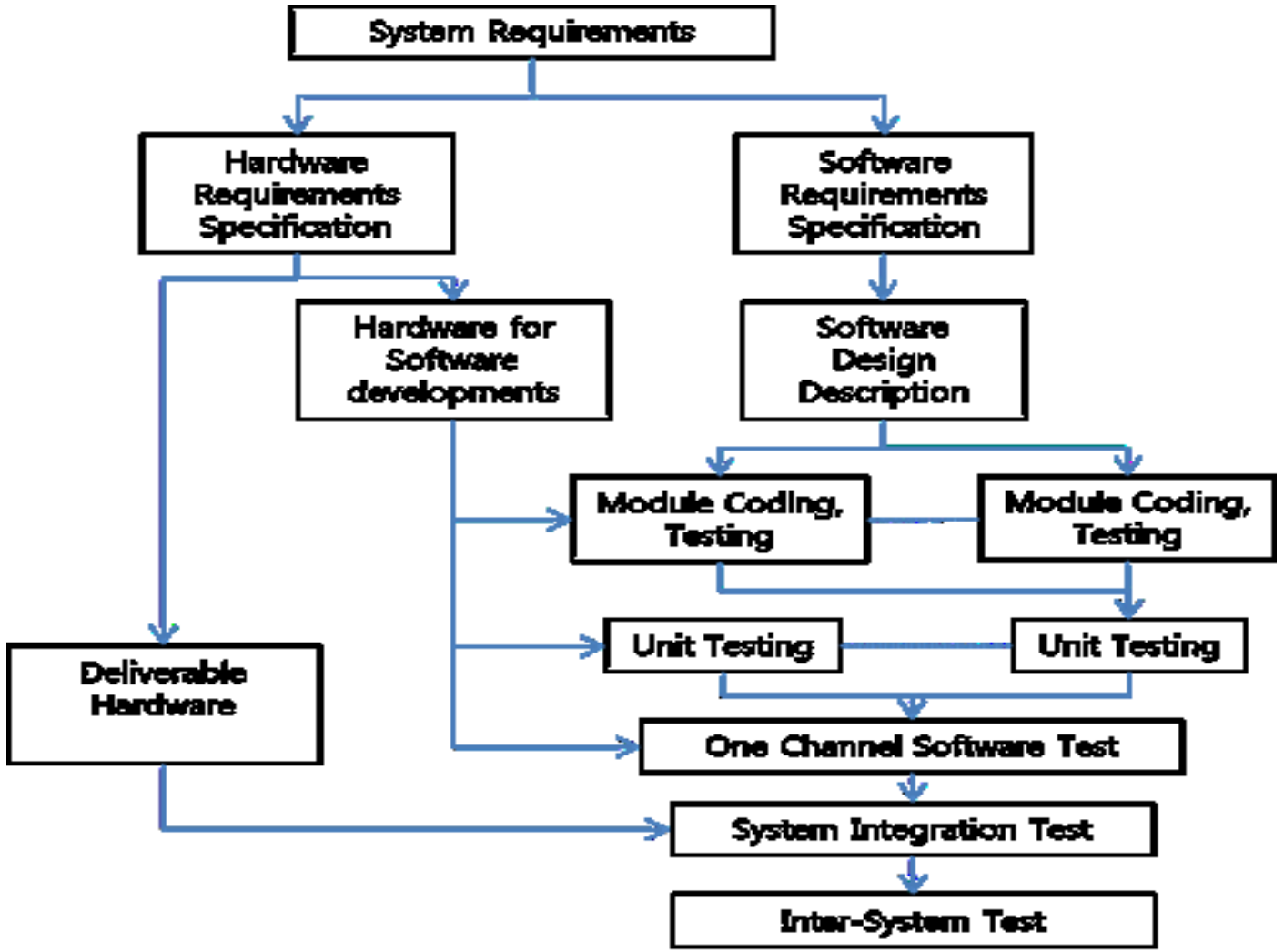
2.3 PPS Software V&V (1/2)

- The software Verification and Validation (V&V) has been performed to meet the regulatory requirements and standards such as IEEE 1012.
- The software is classified into four different classes based on the criticality of the software assigned for the system.
- PPS software in PLC performing safety function is classified as safety critical class which corresponds to SIL 4 in IEEE 1012.
- V&V is performed by independent engineering group.
- V&V group performs document verification, requirement traceability analysis, and code review during development phase.
- After completion of software implementation by design group, the software is turned over to the V&V group for testing.

2.3 PPS Software V&V (2/2)

- The Module Testing (MT) is performed for every module to meet the branch coverage criteria. The test cases are generated using test tool to confirm the branch coverage of 100%.
  - module is loaded into the PPS test hardware to confirm that the execution results are correct during MT.
- The unit testing is performed on a unit program basis. Unit Testing(UT) is executed as a separate task in the processor module.
  - Every functional requirement in the software requirements specification is executed in the unit testing.
- 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.
  - CPU overloading conditions are exercised.
  - The man machine interface of the display output is tested for correct display.

Software Testing Scheme



2.4 PPS Software Test Results (1/3)

- The PPS software were released for V&V 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)
- 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.

2.4 PPS Software Test Results (2/3)

- 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 for consistency and user's request in addition to findings in TERs.
- To implement these changes, SCRs (Software Change Request) were issued.
- There have been
  - 182 SCRs in 2012,
  - 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.

2.4 PPS Software Test Results (3/3)

- The corrections 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 software errors related to the display and diagnostics were found 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 disadvantages of the waterfall model life cycle is clearly shown by the number of corrections that has occurred to improve MMI aspect of the system display.
- it might be better to adopt rapid prototype model for the display software and introduce human factor engineering V&V in parallel.