Software V&V of PPS for Shin-Hanul Nuclear Power Plant Units 1&2

Cheollak Park, Dongpa Kang, Changhui Choe, Sedo Sohn, Seungmin Baek
KEPCO Engineering & Construction Company, Inc., 150 Deokjin-dong, Yuseong-gu, Daejeon, 305-353

1. Introduction

Software V&V processes determine whether the development products of a given activity conform to the requirements of that activity and whether the software satisfies its intended use and user needs. This paper introduces the software V&V activities and tasks performed during the software development life cycle of the Plant Protection System (PPS) for Shin-Hanul Nuclear Power Plant Units 1&2 (SHN 1&2).

The PPS generates signals to actuate Reactor Trip (RT) and Engineered Safety Features (ESF) whenever monitored processes exceed predetermined limits, and the PPS software is classified safety critical and an independent V&V is thus required according to regulations, code and standards [1-4].

2. Details and Results

In this section software V&V activities and tasks of PPS are described according to each of software development life cycle phase.

2.1 Concept phase

The concept documents such as contract, system design requirements, design specification were reviewed for consistency and incompatibilities, and allocation of functions to hardware and software items were also assessed. The preliminary software hazard analysis was performed to evaluate the potential impact of plausible software failure on identified hazards. The outcome of the concept verification activities was incorporated in the requirements phase report.

The plan documents such as software V&V plan, QA plan and software safety plan, and preliminary software hazard analysis were produced as outputs of this phase.

No	Name	Hazard Description	Hazard Cause	Method of Detection	Potential Consequences	Safety Hazard Mitigation	Safety Hazard Control Verification Method
1	Bistable Processor	Numerical value below acceptable range	Entry error in converting raw signals to engineering units or hardware read errors	Range limit check, system diagnostics	Channel trip	4 channel redundancy, channel trips on input out-of-range For CMF of all channels, system trip/actuation on out-of-range	Software code inspection, testing and system validation test
2	Bistable Processor	Numerical value above acceptable range	Entry error in converting raw signals to engineering units or hardware read errors	Range limit check, system diagnostics	Channel trip	4 channel redundancy, channel trips on input out-of-range For CMF of all channels, system trip/actuation on out-of-range	Software code inspection, testing and system validation test
3	Bistable Processor	Bistable process value inputs out of range	Hardware error	Range limit check, system diagnostics	Channel trip	4 channel redundancy, channel trips on input out-of-range For CMF of all channels, system trip/actuation on out-of-range	Software code inspection, testing and system validation test
4	Bistable Processor	Numerical value within range, but wrong	Entry error in converting raw signals to engineering units or hardware read errors	Intra/Inter channel comparison failure	No trip when it is required	4 channel redundancy, DPS for software CMF	Software code inspection, testing and system validation test
5	Bistable Processor	Numerical value has wrong physical units	Programming error	Intra/Inter channel comparison failure, Administrative inspection	Inadvertent channel trip or failure to trip when required	DPS for software common mode failure affecting both bistables in multi channels	Software code inspection, testing and system validation test of DPS
6	Bistable Processor	Numerical value has wrong data type or data size	N/A	N/A	N/A	POSAFE-Q standard product does not allow mixing of data size	N/A
7	Bistable Processor	Non-numerical value incorrect	Programming error	Intra/Inter channel comparison (by visual inspection) failure, System diagnostics	Inadvertent channel trip or failure to trip when required	4 channel redundancy, DPS for software CMF	Software testing

Fig. 1. Preliminary software hazard analysis

2.2 Requirements phase

The system and software requirements verification of functional, performance requirements and external interface requirements were performed. These requirements were verified by conducting requirements traceability analysis between the System Requirements Specification (SysRS) and Software Requirements Specification (SRS) as described in Fig 2. DOORS tool has been used to conduct the Requirements Traceability Matrix (RTM) during all the software development life cycle phases. The test plan also was prepared for testing.

The phase V&V report, RTM and test plan were produced as outputs of this phase.

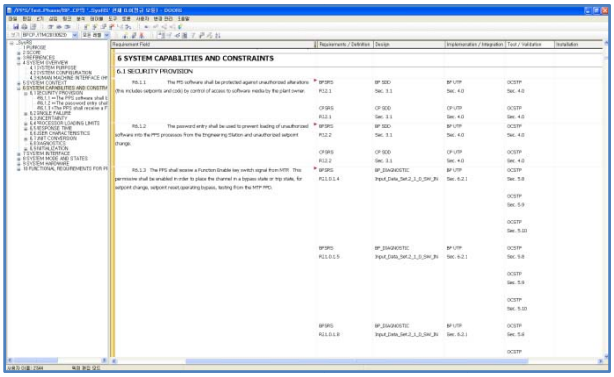

Fig. 2. RTM made by using DOORS tool

2.3 Design phase

The requirements verification review was performed to ensure that the software requirements were reflected properly on the Software Design Description (SDD) which provides sufficient design details to support a code development. This verification was performed through conducting the requirements traceability analysis between the SRS and SDD.

The phase V&V report and RTM were produced as outputs of this phase.

2.4 Implementation phase

It was verified and validated that the SDD was transformed into code, database structures, and machine executable representations correctly. First of all, the code inspection was performed to verify that the source code conformed to applicable coding guideline. Secondary, the module testing was performed to validate each module consisting of custom function block elements against the requirements specified for

that module. The structural testing referred to as a White Box testing was performed to measure the coverage of module, and LDRA tool was used for this testing. The test result was made as a report shown in Fig.3. After structural testing, the functional testing referred to as a Black Box testing was also performed to determine whether the functional requirements of module were met. Finally, the unit testing was performed for a complete software program consisting of multiple modules under target equipment [5].

The phase V&V report, RTM, code review report, module/unit test procedure, module test case and module/unit test report were produced as outputs of this phase.

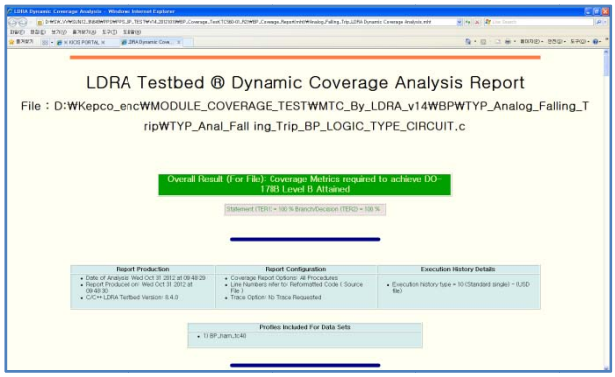

Fig. 3. Coverage analysis report of LDRA tool.

2.5 Test phase

The system functional and performance requirements allocated to software were validated by execution of one channel software testing. The one channel software testing was performed under the Development Facility (DF) consisting of two (2) Bistable Processors (BPs), three (3) Coincidence Processors (CPs), Interface and Test Processor (ITP), and Operator Module (OM)/ Maintenance & Test Panel (MTP). The DF configuration is identical to the Channel D of the deliverable PPS. During this testing, the I/O simulator was used for generating all analog, digital inputs and incoming SDL links [5]. In one channel software testing, the functional requirements of normal mode, test mode and failure mode, and response time requirements from the input of the bistable processors to the output of initiation relays specified in SysRS were validated.

The phase V&V report, RTM, one channel test procedure and one channel test report were produced as outputs of this phase.

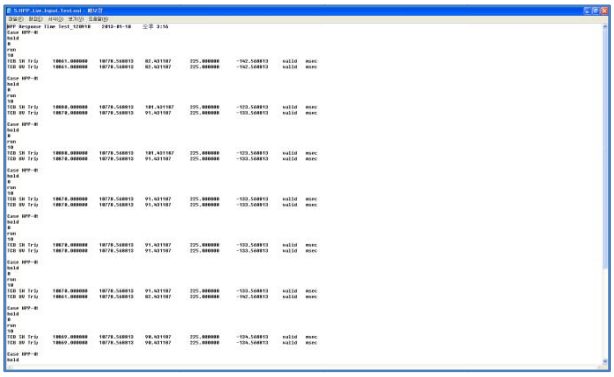

Fig. 4. Response Time Test Result File.

2.6 Installation and checkout phase

The correctness of the software installation in the target environment is to be verified and validated by utility.

The V&V task to be performed is to grant the code certificate when the PPS software is completely verified and validated, and the final software V&V report including code certificate, final RTM and final software hazard analysis will be produced as outputs of this phase.

3. Conclusions

The software V&V efforts, sufficiently disciplined and rigorous, are quite essential to demonstrate that the software development process is of a high quality.

The software V&V of PPS for SHN 1&2 has been accomplished successfully with systematic V&V procedures and methods established until test phase in compliance with related code and standards. In particular, the use of automated tools such as LDRA and DOORS greatly has contributed to an improvement of a software quality, and a reduction of a verification time and human errors.

REFERENCES

[1] Reg. Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”, USNRC, 2006.
[2] Reg. Guide 1.168, “Verification, Validation, Review, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants”, USNRC, 2004.
[3] IEEE Std. 7-4.3.2, “IEEE Standard for Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, 2003.
[4] IEEE Std. 1012-1998, “IEEE Standard for Software Verification and Validation”, 1998.
[5] Dongpa Kang, Cheollak Park, Changhui Choe, Sedo Sohn, Seungmin Baek, “The Software Testing of PPS for Shin-Ulchin Nuclear Power Plant Units 1 and 2”, KNS Oct 25-26, 2012.