Society for Science and Education
United Kingdom

TMLAI Transactions on
Machine Learning and Artificial Intelligence

Volume 2, Issue 6
ISSN: 2054 - 7390

# The Modernization of Feed Water Pump Turbine (FWPT) Controller for Nuclear Power Plants Unit 5 and 6

**Kwangyoung SOHN, Jayoung LEE and Changhwan CHO**
*Mirae-en, Daejeon, Republic of Korea*
kwangyoung.sohn@mirae-en.co.kr

## ABSTRACT

For modernization, Feed water Pump Turbine (FWPT) for HANUL Nuclear Power Plants Unit 5 & 6 has been replaced with Triple Modular System including the upgrade of control logic actuating Low Pressure/High Pressure (LP/HP) stop valves and control valves. This modernization includes hardware platform change as well as ladder logic changes. This paper provides the lesson learned from the design support and the verification and validation (V&V) for control logic software in accordance with IEEE 1012[1], which describes the Software Development Life Cycle (SDLC) phase activities for independent verification and validation (V&V). As usually it is necessary to interpret standards by upward and/or downward tailoring, i.e. interpretation, based on the SIL level and application function for practical independent V&V. It has been conducted to list up the inspection viewpoints for software itself as well as architectural design including the hardware interfaces. For successful independent V&V of FWPT, the specific viewpoints and approach are employed according to the functional characteristics and code optimization. The V&V for this project reviews only the requirement, design, implementation, and test phase. This article also provides the difficulty experienced during independent V&V including the design support, and concludes by addressing a couple of lessons learned for FWPT V&V.

Keywords: FWPT (Feed water Pump Turbine), Software Development Life Cycle (SDLC), Verification and Validation (V&V), Nuclear Power Plant (NPP)

## 1 Introduction

Due to the hardware aging and obsolescence, the upgrade of FWPT for HANUL nuclear power plants unit 5 & 6 was brought up as necessary. In the course of upgrade, independent V&V has been requested to validate the design integrity of the software and its system which is classified to safety-related in accordance with the organization as Figure 1.

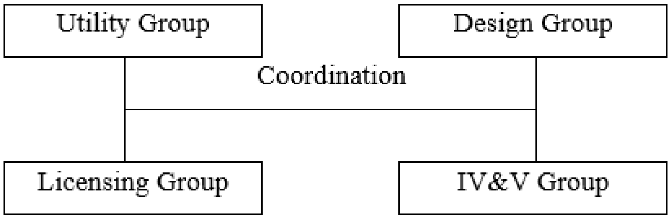

**Figure 1: The Organization for FWPT V&V for HANUL NPP unit 5 & 6**

**DOI:** 10.14738/tmlai.26.386
**Publication Date:** 13th December, 2014
**URL:** http://dx.doi.org/10.14738/tmlai.26.386

For the transparency of V&V activity, the design team and review team is officially separated for managing the independent review of the system and the component design, which is also the requirement from licensing organization of Korea Institute of Nuclear Safety (KINS) shown in Figure 1.

However IEEE 1012 code is generally conceptual that is applicable to all the software of various fields including FWPT, it is necessary to devise application-specific review points to V&V team, which might be enhancing the reliability of the FWPT software system.

## 2 FWPT Overall

The critical characteristics[8] for FWPT is straight forward, i.e., processing the sensor signals, process engineering con-version, send out the result to monitor and control the Low Pressure/High Pressure (LP/HP) stop valves and control valves.

Figure 2 indicates the interconnection diagram between FWPT and other auxiliary systems which provide the process input and control output. The main function (critical characteristics) of FWPT is to control the turbine output by manipulating the stop and control valves for Feed water Pump.

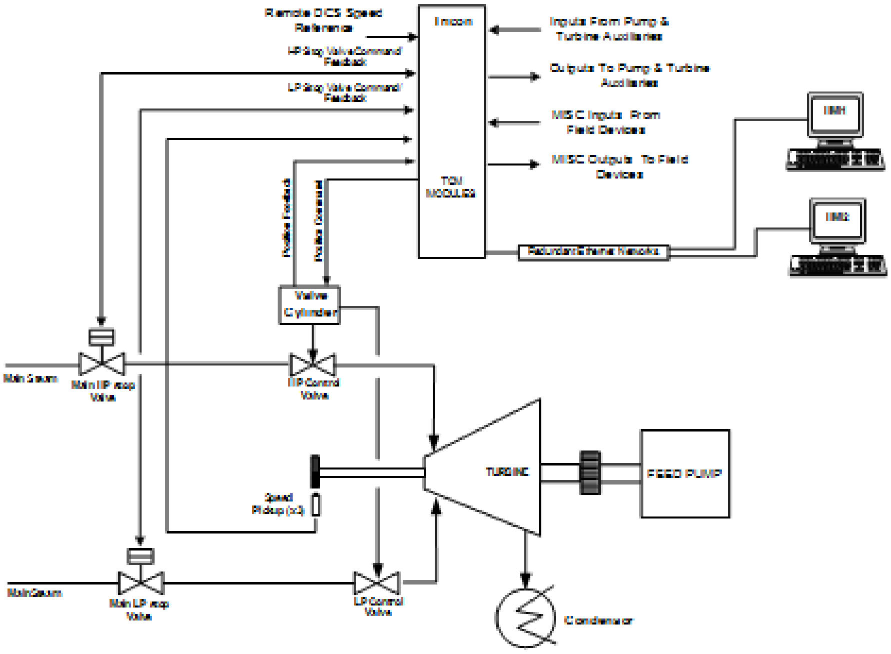
Remote DCS Speed Reference
HP Stop Valve Command/ Feedback
LP Stop Valve Command/ Feedback
Tricon
TCM MODULES
Inputs From Pump & Turbine Auxiliaries
Outputs To Pump & Turbine Auxiliaries
MISC Inputs From Field Devices
MISC Outputs To Field Devices
HMI1
HMI2
Redundant Ethernet Networks
Position Feedback
Position Command
Valve Cylinder
Main Steam
Main HP stop Valve
HP Control Valve
TURBINE
FEED PUMP
Speed Pickup (x3)
Main Steam
Main LP stop Valve
LP Control Valve
Condenser

Figure 2: FWPT for HANUL unit 5 & 6

Input and output for FWPT that is controlling LP stop/control valve and HP stop/control valve simply is composed of triple sensors and signal processors. These signals are processed by the algorithm in each triple processor. Also one of the final outputs of triple modules is selected as a result of voting for actual actuation of valves by comparing the speed values from the magnetic speed pick-up devices...

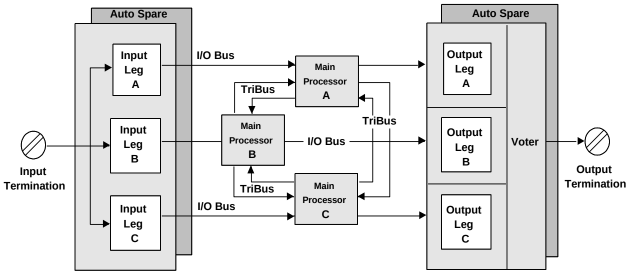

Figure 3: Triple modular software structure

Figure 3 provides the general configuration of the FWPT system including hardware and software. A single input and output is divided into 3 inputs and outputs for FWPT, which are processed in each hardware. And those signals are processed in the triple processor (PLC) for calculation and PID control.

# 3 Approach for FWPT V&V

## 3.1 Identification of critical characteristics

FWPT software on HANUL 5&6 is independently verified and validated. Based on the conceptual V&V activities of IEEE 1012, the major viewpoint is selected as below through the system function and performance analysis.

1. Identification of the critical functional characteristics for the FWPT – controlling LP/HP stop and control valves
2. Identification of the interface between the internal and external sub-components like the communication and its transmission frequency (including the serial data links) – interface through HMI (Human-Machine Inter-face)
3. Identification of the performance characteristics – response time for actuating valves
4. Identification of the appropriateness on the functional cohesion and coupling in final implementation [2] – decomposition of logic module
5. Identification of the test coverage – test plan for a type of test
6. Exceptional handling

The following section will address the detail of the several item enumerated above, and difficulty that has been experienced during independent verification and validation and design support.

## 3.2 Modified verification and validation

The verification and validation team has been organized to meet the independencies of managerial and technical aspect. However the team is not independent from the financial budget, which means there is a decisive weakness for performing a sincere verification and validation. See Table 1 for independency for this project.

## 3.3 Identification of the interface

For the modernization of FWPT controller, some of the hardwired interconnections between components are connected through a communication network. When communication is used for data exchange, there might be a discontinuity of data when a network failure occurs and is recovered soon again. Through these communication media, the data pertaining to FWPT control and monitoring is sent out to MCR and relevant human interface.

### 3.4 Identification for performance characteristic

FWPT could have a malfunction mainly caused not by human intervention error but by internal software malfunction. Because the human intervention is limited to the manipulation of hand switch for MANUAL/AUTO transition, and the determination of a series of set points. This could result in critical hazard of malfunction in controlling the turbine in the type of human errors.

### 3.5 Cohesion and coupling

It is the design verification to check if the software module is decomposed to be constructed well based on the logical function decomposition, getting rid of implementation complexity and ambiguity resulting from incomplete software design. It is a critical measure to judge the testability and maintainability of software [2].

### 3.6 Reliability of function and performance

It is a new aspect of verification and validation to check if the function to be implemented is implementable in a new software logic composer or hardware. Recently most of functions, even implemented with hardware in a legacy plant, are reformed as software, targeting for a digital system. Also hardware on which the software is running is different from the legacy hardware, and also the legacy code is transformed into a different algorithm although upgraded algorithm is implemented to be functioning in the same way to legacy code. It is very important check point to verify that the function and performance is equivalent to legacy.

### 3.7 Exception handling

In any software function, there is an exception of partial function. This partial function shall be clearly designed and implemented, which supports a reliable test plan and procedure in the test phase. But in this project, it is found that the software is functioning by assuming the prefabricated route, which means this is not resilient to the exceptions.

### 3.8 Test coverage

Practically exhaustive test coverage is not desirable and not recommended for robust software testing. However, when the output of the software is actuating the hardware devices connected to system, the maximum test coverage is recommended in test. For this, systematic and concrete test coverage has been generated by designer as well as independent verifier and validator based on the 6 criteria in Section 2.1. It was very helpful to remove the delicate failure sources, and it becomes the solid basis of test procedure preparation.

## 4 Lesson learned in FWPT V&V

The following are the patterns found through the analysis of anomaly reports in each phase about FWPT in HANUL nuclear power plant unit 5 & 6.

## 4.1 Requirement refinement

In case of this project, there has been only the legacy source code and control logic which could be source of SDLC documentation. Based on this limited source, Software Requirement Specification (SRS) and Software Design Specification (SDS) have been prepared. So it omitted the some of the requirements, which have been finally resolved through anomaly report and analysis, and there was feedback for this to design documents. In requirement extraction on legacy plants without complete design data, it is necessary to discuss requirement refinement. As noted in [8], the inception phase of design is very critical for further process of SDLC. Some of the requirement has been identified in the design phase, not in requirement phase, which has been reincorporated into the design by iteration.

## 4.2 The Code optimization in implementation

The code analysis as well as decomposition analysis such as cohesion and coupling have been conducted for software integrity and completeness. The following is one of the example for this

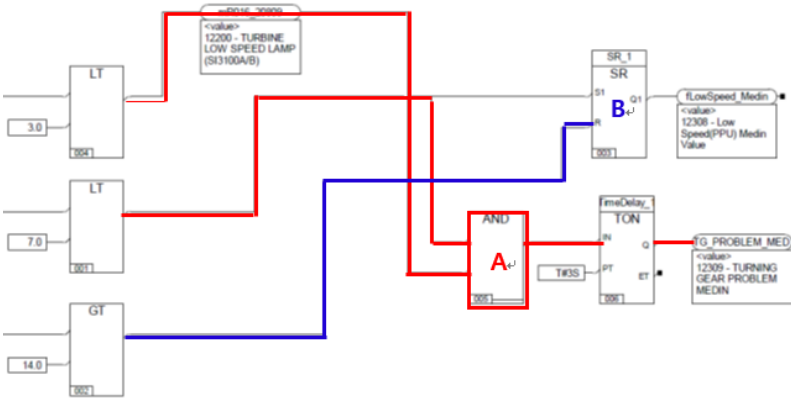

Figure 4: logic diagram for optimization

In figure 4, the input value is less than 3.0, then the block “A” has a meaning to generate the effective output, i.e. 1. Thus without AND gate logic it is possible to generate the trigger condition by comparing that input is less than 3.0. This is one of the examples that the optimization is required as necessary, which means that the developer does not fully understand the requirements.

## 4.3 The management of V&V

According to Annex C “definition of independent V&V” of IEEE 1012-2004[1], independent V&V is categorized by three parameters: technical independence, managerial independence, and financial independence as described in Table 2.

Table 1: Independent verification and validation form

| Independent V&V Form | Technical | Management | Financial |
|---|---|---|---|
| Classical | I | I | I |
| Modified | I | i | I |
| Integrated | i | I | I |
| Internal | i | i | i |
| Embedded | e | e | e |
| *FWPT project* | *i* | *I* | *e* |
| NOTE<br>I : Rigorous,<br>i : Conditional Independence,<br>e : Minimal Independence | | | |

However FWPT project has the variance deviating from the independency from IEEE 1012. For reference, Korea Hydraulic and Nuclear Power (KHNP) has changed the project verification structures in hardware qualification into CLASSICAL form by reinforcing the internal regulation but still no action for software verification and validation.

### 4.4 Test environment

Unit testing and integration testing is for verifying its function and performance only. However Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) should integrate the hardware and/or peripheral interfaces with software itself, which is ultimately an architectural system design testing for FWPT for HANUL unit 5 & 6. In this project, verification and validation should have considered the complete integration with hardware interfaces, but it was incomplete in integration.

### 4.5 Design data freeze

As we're well aware of that the process for verification and validation is to review the SDLC design data in each phase right after the issue of frozen design data of each phase. But the design data such as SRS, SDS, source code and a multiple of test procedure that had not been finished and signed appropriately were transmitted to verification and validation organization, which brought up repetitive review process wasting a time. Thus the verifier has felt the difficulty in conducting the review process, i.e., entailing the repetitive review process for a single design documents like SRS, SDS, multiple test procedure and source code. For verification and validation team it seemed to have been an activity to support the fundamental design work, not verification and validation work. Also there has been case that utility changed the requirement in the implementation and testing phase all of sudden.

### 4.6 Anomaly resolution process

This is not a technical issue but a managerial issue for verification and validation process. Once verifier finds out the anomaly for target system regarding function, performance and interfaces, these anomaly report should have been justified and resolved by the designer with feedback to FWPT design selectively and appropriately.

## 5 Conclusion

Through the independent verification and validation for FWPT in HANUL nuclear power plant 5 & 6, a couple of obstacles in conducting the verification and validation have been found practically.

In this project, the selection of critical characteristics of FWPT was very important even though some of the requirements are found in phase later than requirement phase. Also it is found that the requirement refinement, code optimization, the management of independent V&V, test environment, design data freeze, and anomaly resolution process is one of difficulty in performing successful verification and validation.

Among them, the design data freeze, anomaly resolution process and design support due to the lack of understanding of FWPT system have been a tiresome factors deteriorating the smooth and successful independent verification and validation.

Once the completion of independent V&V, issuing the anomaly report, a resolution meeting between independent verifier and validator and designer to obtain the optimal solution should have been held in every SDLC phases. Unfortunately there is a tendency that the designer will not partly accept the anomaly issued just because the function is any-way performed well even though there is room for optimization and documentation [8].

To be a successful independent verification and validation, it is important to make an effort to find out the technical anomaly as well as to cooperate each other, i.e., designer and validator.

## ACKNOWLEDGEMENTS

This work has been conducted with the support of INVENSYS Korea, especially thank to director Myung. Soon. Kim.

## REFERENCES

[1]. IEEE Std 1012™, “IEEE Standard for Software Verification and Validation”, 2004

[2]. Roger S. Pressman, Ph. D, ISBN 0073655783, “Software Engineering, A Practitioner's Approach”, Fifth Edition, McGraw-Hill Higher Education.

[3]. Kyung Ho Cha, Kee Choon Kwon, Chun Se Woo, “The software verification and validation tasks for a safety critical system in nuclear power plants”, International journal of safety, vol.3 no.1, pp.38-46, 1598-7302, 2004.

[4]. C. Ponsard, P. Massonet, J. F. Molderez, A. Rifaut, A. van Lamsweerde, H. Tran Van, “Early verification and validation of mission critical systems”, Formal Methods in system Design, Volume 30, Number 3, pp.233-247, 0925-9856.

[5]. IEEE 829, “IEEE Standard for Software and System Test Documentation”, 2008

[6]. ANSI/IEEE 1008, “IEEE Standard for Software Unit Testing”, 1987

[7]. NUREG/CR-6430, “Software Safety Analysis”, 1995

[8]. Lessons learned from Practical Independent Verification and Validation based on IEEE 1012, A Journal of Software Engineering and Applications, JoonKu LEE, YangMo KIM