Validation of Plant Control System Design Change

Dongil Lee [a*]
[a]*KHNP, Central Research Institute, 70, 1312-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, South Korea*
[*]*Corresponding author: diturtle@khnp.co.kr*

1. Introduction

There are many different types of Nuclear Power Plants (NPPs) in Korea. There are many NPPs that have started generating energy since the 1990s. The 1990s is a very important time. This is the point at which the digitization of facilities in NPPs began.

The digitization of facilities has taken place in various systems. From the Plant Control System (PCS) and Turbine Control System (TCS) to the current Man Machine Interface System (MMIS), it is becoming more advanced and rapidly replaced.

The initial model of digital NPPs is the PCS in Hanul-NPP units five (5) and six (6). PCS is a facility that controls and monitors safety and non-safety power plant equipment [1]. The function and scope of PCS are very important and extensive, so when an error occurs, it greatly affects the safety and operation of the NPP.

PCS, which is a very important facility, often undergoes design changes to enhance safety and for various reasons. In this paper, the validation of the logic of the design change of the PCS facility and, the newly introduced nuclear Control Logic Diagram (nCLD) for Hanul-NPP units five (5) and six (6) will be explained.

2. Design Change of PCS

2.1 Background of PCS Design Change

PCSs are Hanul-NPP units three (3) to six (6) Hanbit-NPP units five (5) and six (6), ShinGori-NPP units five (5) and six (6), and Shinwolseong-NPP units five (5) and six (6), which are Optimized Power Reactor (OPR) 1000 NPP.

PCS design changes sometimes reflect design changes of other NPPs, and sometimes change themselves.

2.2 Subject of PCS Design Change

PCS design changes include hardware (wiring) design changes and control logic (hereinafter referred to as software) changes.

Hardware design change is a case of changing the wiring without changing the software of the control device.

Software change corresponds to address change of the communication network or logic change.

3. Validation of Design Changes

In the case of hardware design change, wiring is redone according to the design change document and performance test is completed.

However, since software changes are logic changes, software Verification and Verification (V&V) must be performed. PCS software verification has many differences before and after 2017.

3.1 Software V&V prior to 2017

PCS design changes prior to 2017 were completed with Performance Tests (as System Test) such as hardware design changes. Testing was done through the black-box test Equivalence Partitioning or Boundary Value Analysis (BVA). However, it cannot be said that the test is very unreliable. Various tests were conducted for all possible cases with the efforts of maintenance personnel of Korea Hydro Nuclear Power (KHNP).

3.2 Software V&V since 2017

When a number of problems were issued with electronic cards of PCS, the regulatory body requested that software verification be continuously strengthened from 2016. In 2017, KHNP responded quickly to the needs of the regulatory body, and established guidelines for software verification by referring to IEEE 1012-2004 and IEEE 1219-1998.

IEEE 1012-2004 describes software V&V for all processes of software, and IEEE 1219-1998 describes software verification that occurred during maintenance [2,3].

The purpose of the developed software V&V guideline is to prepare a software V&V plan before performing performance tests, verify design documents, and perform unit tests before performance tests according to the plan to verify the logic of software in the laboratory.

Unlike performance tests, unit tests are very sophisticated and systematic.

3.3 Software V&V Method

Verification of safety and non-safety design changes is carried out by KHNP's Central Research Institute (CRI) or Task Force Team (TFT) at NPPs, which is independently reviewed by a third party.

The independent software V&V team reviews the design documents and prepares the software V&V plan. The software test plan of the software V&V plan designs and executes the test by applying the regression testing technique to the changed software.

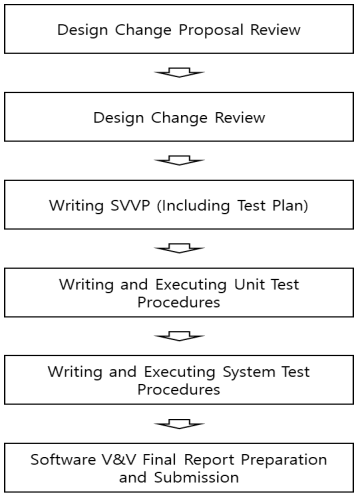

Fig. 1. Software V&V Procedure

Unit Test considers the characteristics of control logic and tests by applying Equivalence Partitioning and BVA methods to Test cases. The coverage of the test is aimed at 100% execution to the extent possible.

The performance test applies the software to the actual equipment and performs the same test as before. When all unit/performance tests are completed, a final report is prepared, and the document is submitted to the regulatory body.

4. Limitations and Overcoming of Unit Tests

4.1 Limitations of Unit Testing

The unit test of PCS is tested on a hot-panel, and the performance test is performed on an actual facility. However, not all tests are available on the hot-panel. In this case, the test is performed after bypassing the signal of the field facility.

In actual facilities, various tests are difficult due to limitations on input. In addition, it is not possible to know the input change or output of the signal inside the software in the test on the hot-panel or actual equipment.

4.2 Overcoming the Limitations of Unit Testing

To overcome the limitations of unit testing, KHNP developed a software called nCLD. It is possible to virtually input the control logic signal and measure the intermediate signal and final output of the control logic.

Signal input/output is possible in real time, and it is verified in three (3) ways: highlight, timing diagram, and truth table [4].

Fig. 2. Three (3) types of Simulation

5. Conclusions

After strengthening the software V&V since 2017, there has been no power generation stoppage due to problems with the control logic of PCS.

In addition, nCLD, which was recently developed and introduced to Hanul-NPP units five (5) and six (6), made it possible to accommodate all test techniques for unit tests of software V&V.

[1] D.G. Kim, K.I. Shin, M.J. Choi, Plant Control System (PCS) Communication Reliability Analysis for Ulchin Nuclear Power Plant 5&6, Power Engineering, Volume 16, p42, 2005.
[2] IEEE Computer Society, IEEE Std 1012 for software verification and validation, 2004.
[3] IEEE Computer Society, IEEE Std 1219 for Software Maintenance 1998.
[4] D.I. LEE, Development of Digital Control Logic's Verification Technology based on Artificial Intelligence, Conference on Information and Control Systems, p397-398 ,2020.