IMPLEMENTATION OF VERIFICATION AND VALIDATION FOR REPLACEMENT OF HANARO CONTROL COMPUTER

Hyung Kyoo Kim*, Min Woo Lee, Yeong San Choi, Yun Taek Yim and Hoan Sung Jung

Korea Atomic Energy Research Institute
111 Daedeok-daero 989beon-gil, Daejeon, Korea

ABSTRACT

In the development of a computer based system, it is important to assess if the system meets the requirements and specifications, and if its final outputs are correct. Software verification and validation (V&V) is the process of checking whether a software meets the requirements and ensuring that the software satisfies the intended purpose and user needs. HANARO (High-Flux Advanced Neutron Application Reactor), which is an open-tank-in-pool type research reactor with 30 MW of thermal power, achieved its first criticality in 1995. Recently, there has been a fast development in the field of electronics. Many manufacturers of I&C equipment or components have disappeared or merged with others. The HANARO reactor control computer, which is a programmable controller system called a Multi Loop Controller (MLC) manufactured by MOORE (Canada), had been utilized for 20 years after its initial criticality. However, its supplier no longer produces the required components and disappeared from the scene, and thus support for this system can no longer be guaranteed. With a refurbishing plan of control computer, its replacement was completed successfully in 2015. The control algorithm has been migrated into a new control computer system. Implementation of V&V has been committed on the basis of IEEE Std. 1012, which was issued in 2004; and the Software Development Life Cycle (SLDC) framework consists of seven phases: planning, requirements, design, implementation, test, installation and checkout, and operation and maintenance. This paper describes the V&V activities implemented for the replacement of the HANARO control computer.

1. INTRODUCTION

In the development of a computer-based system, it is important to be able to determine and assess if the system meets the requirements and specifications, and if its outputs are correct. Faults can lead to system failures causing public hazards, financial loss, or property damage, as well as a deterioration in the reliability of the system. Early detection results in a better solution than quick fixes. The purpose of V&V is to help the development organization build quality into the system during its life cycle. The V&V processes provide an objective assessment of the products and processes throughout the life cycle [1]. The V&V is carried out in parallel with the software/system development process to find and correct errors in the development life cycle as early as possible. A Software Verification and Validation Plan (SVVP) is required for software applicable on a computer-based control system and shall specify the activities to be performed during the software management and development process in accordance with IEEE 1012. The V&V activities include analysis, evaluation, review, inspection, assessment, and testing conducted by a competent person or group. IEEE 1012 describes the SDLC phase activities for software V&V including Independent Verification and Validation (IV&V) for nuclear power plants in a truly general and conceptual manner, which requires the upward and/or downward tailoring on its interpretation for practical V&V. It contains crucial and encompassing check points and

guidelines to analyse the design integrity, without addressing the formalized and specific criteria for IV&V activities confirming the technical integrity.
The MLC has been used to control and regulate HANARO since 1995. However, the supplier did not produce the MLC, and thus the ageing, obsolescence, and a short supply of spare parts have caused great problems. The refurbishing plan of the control computer was established in 2009, and its replacement was successfully completed in 2015. The goal of the refurbishment program was a functional replacement of the reactor control system in consideration of suitable interfaces, compliance with no special outage for installation and commissioning, and no change in the well-proved operation philosophy. The new HANARO Control Computer System (HCCS) is a Discrete Control System (DCS) using PLC manufactured by RTP. The architecture of HCCS is shown in Fig. 1. The software V&V was conducted in order to assess whether the new control system is consistent with the specifications and requirements.

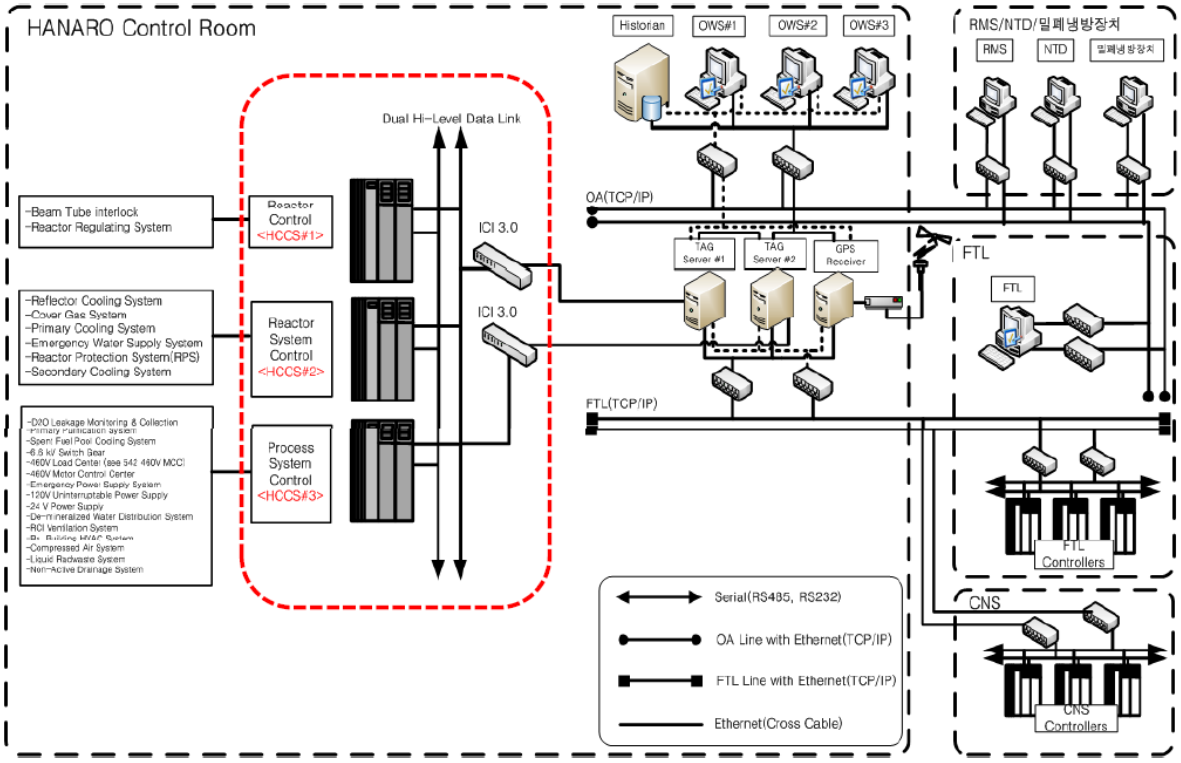

Figure 1. Architecture of HCCS

2. SOFTWARE VERIFICATION AND VALIDATION OF HCCS

2.1 Overview of Software Verification and Validation

V&V is one of the software engineering disciplines for improving the quality of the system during the development process or during the life of a computer-based system. IEEE 610 defines the verification and validation as follows [2]:

- Verification: The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase.
- Validation: The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies the specified requirements.

The verification process provides objective evidence for whether the products perform the following:

- Conform to the requirements (e.g., for correctness, completeness, consistency, and accuracy) for all activities during each life cycle process
- Satisfy the standards, practices, and conventions during the life cycle processes
- Successfully complete each life cycle activity and satisfy all the criteria for initiating the succeeding life cycle activities (i.e., builds the product correctly)

In addition, the validation process provides evidence for whether the products perform the following:

- Satisfy the system requirements allocated to the products at the end of each life cycle activity
- Solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions)
- Satisfy the intended use and user needs in the operational environment (i.e., builds the correct product)

While verification and validation have separate meanings, the verification and validation processes are interrelated and complementary, and use the results from each other to establish better completion criteria and analysis, evaluation, review, inspection, assessment, and test V&V tasks for each life cycle activity. Therefore, V&V as an integrated activity provides several benefits [3]:

- Early detection of high-risk error giving the design group to drive a comprehensive solution rather than quick fixes;
- Evaluation of the products solving the “right problem” against software requirements;
- Objective evidence of software and system in compliance with quality standards;
- Provision of information on the quality and progress of the software and system development;
- Support for process improvements with an objective feedback on the quality of the development process and products.

2.2 Software Verification and Validation for HCCS

2.2.1 HCCS Overview

The HCCS is used for the generation of a control rod driving signal and controls the states of all the systems used to operate the reactor safely. The HCCS is connected to field instrumentations such as detectors and sensors, as well as monitors. The operators can access all signals through a man-machine interface, which is the main console of a computer system at the supervision level. The HCCS is composed of three control computers: the Reactor Control System, Reactor System, and Process Control System. Each system is configured in two cabinets, as shown in Fig. 2.

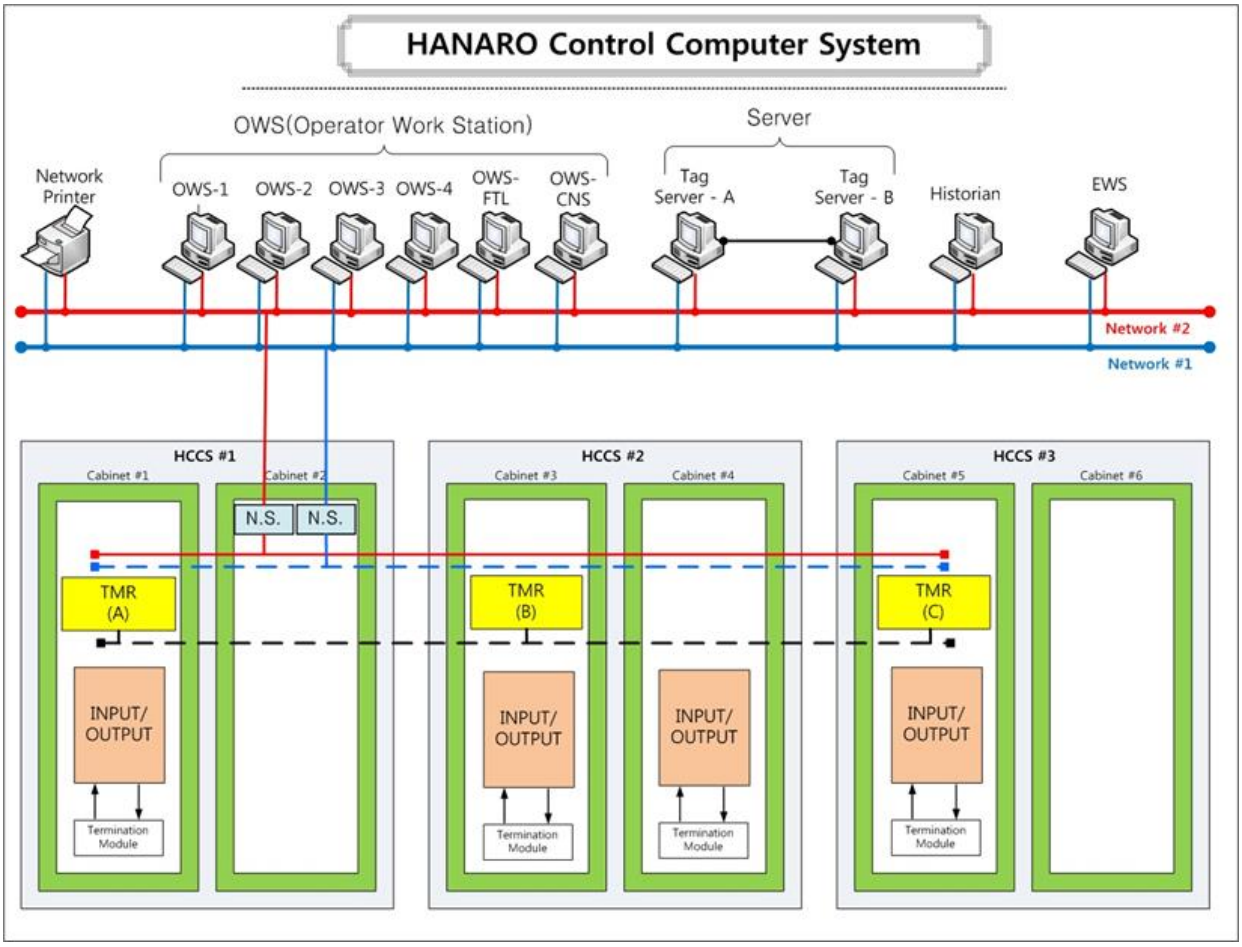

Figure 2. Configuration of HCCS

HCCS consists of triple modular redundant (TMR) processors, and dual redundant I/O modules and power supplies. Fig. 3 shows the configuration of the TMR processors and I/O modules. The TMR processors and dual I/O module will provide high reliability for the following methods:

- Redundant I/O modules run simultaneously, and each I/O module communicates with all processors for signal validation.
- One I/O module communicates with all processors upon failure of a single I/O module.

The HCCS software including firmware was developed to ensure its reliability and completeness through systematic methodologies using a software verification and validation (V&V) program during the software development and implementation processes.

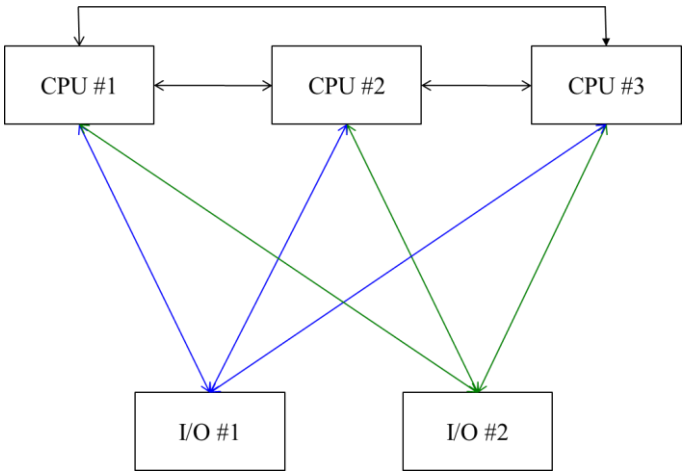

Figure 3. TMR and redundant I/O module

2.2.2 HCCS V&V Philosophy

This section gives an overview of the V&V activities for replacement of HCCS (hereinafter referred to as the HCCS project). Software V&V activities for HCCS was conducted in order to assess whether the new control system meets its specifications and requirements. To determine the minimum V&V tasks for HCCS project, the software integrity level (SIL) was classified based on IEEE 1012.

SIL is a range of values representing the software complexity, criticality, risk, safety level, security level, desired performance, and reliability, and defines the importance of software to the users [1]. The control and regulating system of the HANARO research reactor is important in terms of availability, but is a non-safety system. HCCS software was therefore assigned to integrity level 2. Table 1 shows the classification of the software integrity level.

Software Integrity Level				
Software Program Manual	Safety Critical (SC)	Important to Safety (ITS)	Important to Availability (ITA)	General
Software Integrity Level (IEEE 1012)	SIL-4	SIL-3	SIL-2	SIL-1

Table 1. Software Integrity Level classification

The general philosophy for V&V activities are as follows:

- To ascertain that the control algorithm used at the old control computer will be ported to the HCCS without any changes.
- To simulate the operational conditions using a dynamic test bed for conducting the tests in a practical manner.

- To verify that the new control computer system will not impact other operational systems.
- To conduct V&V by a competent group independent from the design group, as shown in Fig. 4.

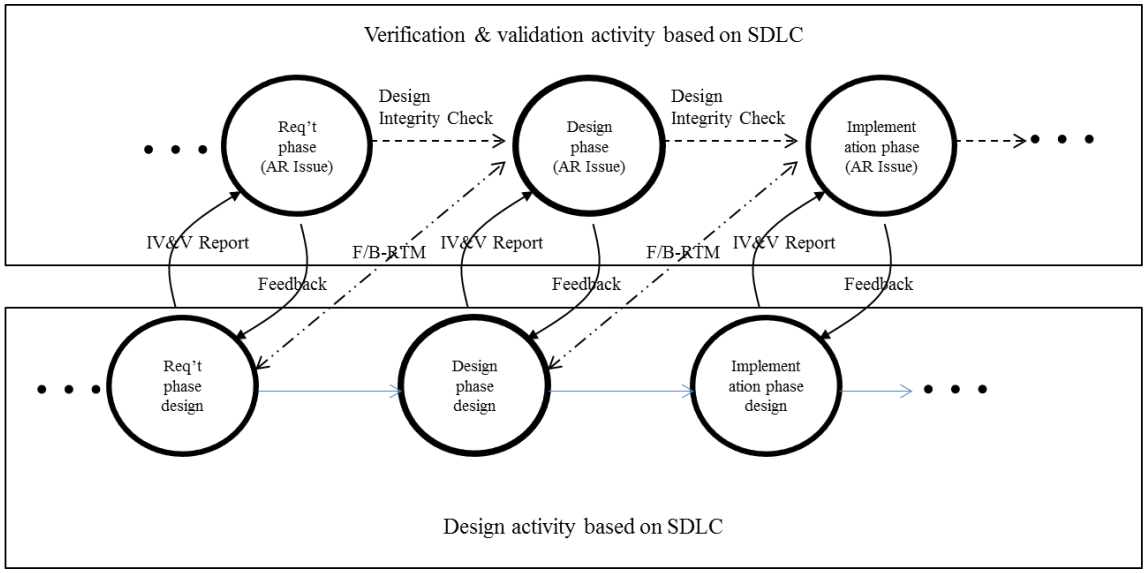

Figure 4. Interface between Design and V&V based on SDLC

2.2.3 HCCS V&V Activities

The software development life cycle (SLDC) for developing HCCS was composed of seven phases: planning, requirement, design, implementation, testing, installation and checkout, and operation and maintenance [4]. A traceability matrix of the critical requirements was established by analysing the identified relationships for correctness, consistency, completeness, and accuracy throughout each phase of the SDLC.

In the planning phase, planning documents for the project, including a software development plan, quality assurance program, V&V plan, and software configuration plan including the cyber security plan and procedure, were established. V&V was performed for the requirements of the installation and checkout among the seven phases of SDLC. Anomalies were also cleared through each iteration of the V&V phase, changes to the program, and testing. The system and software, which were inputs to the V&V, were to be modified for anomaly corrections, quality improvement, or requirement changes in the course of the V&V. When a system or software was modified, additional V&V activities were repeated according to the iteration policy. An evaluation of the cyber security and a risk analysis were conducted while performing V&V tasks by an independent competent group. Table 2 shows the V&V tasks, and the required inputs and outputs, in each phase.

Phase	V&V Tasks	Required inputs	Required outputs
Planning	Stakeholders meeting, Milestone and strategy establishment	Legacy design inputs, project circumstances, existing plan and procedure for software development	Quality assurance plan, Software development plan, V&V plan and procedure, configuration management plan and procedure, cyber security plan
Design	Design evaluation Traceability analysis on software design	SDD	Design V&V report RTM Anomaly report Check list
Implementation	Source code evaluation Traceability analysis on source code	Source code Control logic diagram	implementation V&V report RTM Anomaly report Check list
Testing	Test procedure and report evaluation Traceability analysis on testing	Source code Test plan and procedure Test reports	testing V&V report RTM Anomaly report Check list
Installation and Checkout	Cyber security analysis Risk analysis Installation checkout	Installation package Security and risk analysis report	V&V report including security and risk analysis Anomaly report

Table 2. HCCS V&V Task

2.2.4 On-site functional test

A safety margin assessment (SMA) of the reactor containment building against earthquakes was conducted after the Fukushima Daiichi accident in 2011, and seismic rehabilitation was mandated as a consequence of the SMA. For this reason, HANARO was not in operation for more than 3 years, so a site acceptance test and on-site functional test have been postponed. The SAT (site acceptance test) and on-site functional test as the V&V task on its operation and maintenance was performed in late 2016 after the seismic retrofitting work was completed. The

test for setback operation, automatic/manual operation and verification of trip parameters described in OLC were conducted.

3. CONCLUSIONS

The HANARO control computer system was replaced with new hardware without a change in the reactor control algorithm. Independent verification and validation were conducted throughout SLDC based on IEEE 1021. The V&V activities were iterated until all crucial anomalies were resolved. The V&V activity on HCCS was completed successfully, and its function was confirmed through functional tests using a dynamic test bed during the V&V activities. The performance, integrity of HCCS were confirmed through the SAT and on-site functional test. Safety, operability and utilization of HANARO research reactor will be increase with successful replacement of HANARO reactor control computer.

4. REFERENCES

1. “IEEE Standard for Software Verification and Validation”, IEEE Std. 1012 (2004)
2. “IEEE Standard Glossary of Software Engineering Terminology”, IEEE Std. 610.12 (1990)
3. Dolores R. Wallace and Roger U. Fujii, “Software Verification and Validation: An Overview”, *IEEE Software*, **May 1989**, pp.10-17 (1989).
4. “Software V&V Plan & Procedure for HCCS”, KHCCS-VV101 (Rev.3) (2014)
5. “Risk Analysis Report on HANARO Control Computer System”, HCRA-PD-RAR-2013080R0 (2013)
6. “Site Acceptance Functional Test Procedure and Report for HCCS”, KHCCS-TP-SPT-001 (Rev.0) (2014 & 2016)