Software V&V for the SDLC of the HANARO Control Computer

Min Woo Lee [a*], Yun Taek Yim [a], Seung Kyoo Doo [a], Yeong San Choi [b], Hyung Kyoo Kim [b], Sung Hyo Lee [b]
[a] *Korea Atomic Energy Research Institute, 989-111 Daedeok-daero, Yusenog-gu, Daejeon 34057, Korea.*
HANARO Management Division.
[*] *Corresponding author: leeme@kaeri.re.kr*

1. Introduction

This paper discusses the V&V tasks according to the software life cycle for the replacement of the HANARO control computer system.

The main purpose of V&V is to develop the logic to control HANARO and to verify whether the developed the logic meets the requirements.

V&V completed verification without discrepancy through repeated testing of the software in accordance with the test procedure after a review and based on a checklist for the possible traceability of each step without any missing requirements.

2. Overview HCCS System

To decrease the unscheduled shutdowns and unstable reactor control owing to the use of an MLC(Multi Loop Controller), which was the old system used to control HANARO (High-Flux Advanced Neutron Application Reactor), the system was replaced with HCCS (HANARO Control Computer System) as the new control system 2015.

HCCS was divided into three big systems: reactor control, the reactor building system, and the process control system. Each control system has two cabinets, as shown in Figure 1.

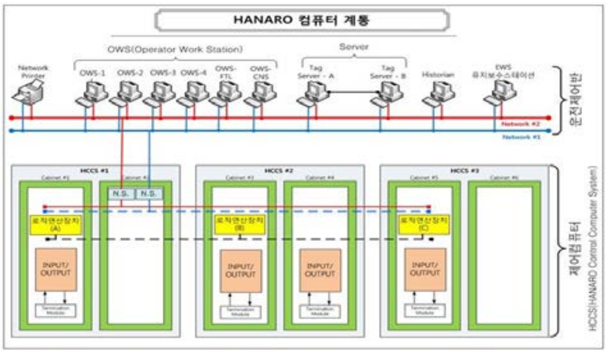

Figure 1. Configuration of the HCCS.

As shown in Fig. 2, it is composed of a triple modular redundant (TMR) programmable controller, dual redundant I/O, and power supply devices in order to increase the safety and reliability during operation. The TMR controller performs the same operation simultaneously, and even though the dual controller fails, a remaining controller will be able to control the entire system without stopping.

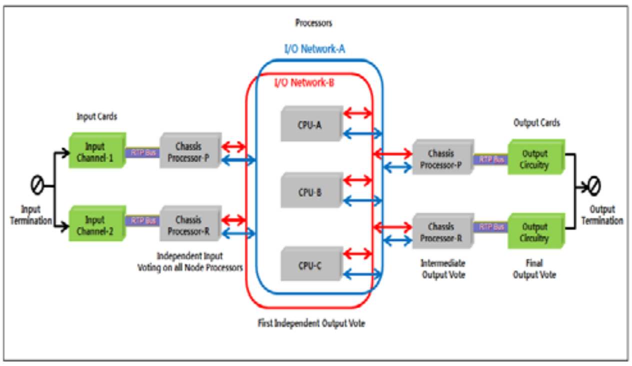

Figure 2. Configuration of HCCS TMR.

It also has a self-diagnostic function, and outputs an LED fault signal during a system failure.

It is also able to analyze the cause of the incident in 1_ms units through the use of the SOE (Sequence of Event) function.

CAR_(Control Absorb Rod) interface devices were designed without changing the existing function. It was designed to operate CAR using the step motor every 200ms communicated with the HCCS.

3. V&V Task

3.1 V&V plan of the SDLC

In the development of the HCCS, a total of 7steps were planned for SDLC_(software development life cycle): planning, requirements, design, implementation, testing, installation, and checking.

In addition, we applied five V&V stages for software verification as shown table 1, based on the SVVP(Software Verification and Validation plan) written through the plan phase according to IEEE 1012-2004.

3.2 V&V for HCCS

SRS was created a total of 22 systems and 471 requirements through the analyzed by PSP(Program specification) of the MLC. In addition, the requirement Phase V&V assessed whether the SRS has been completely generated to meet the performance requirements and traceability.

Table 1. V&V Tasks of HCCS

Phase	V&V Tasks	Required inputs	Required outputs
Requirement	Software requirement evaluation	Technical specification SRS	Requirement V&V Report RTM Anomaly report Check list
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	Risk analysis Installation checkout	Installation package Risk analysis report	V&V report including risk analysis Anomaly report

In particular, we created an RTM_(Requirement Traceability Matrix) for a possible trace with each of the steps shown in table 2.

Table 2. RTM table

No.1	6.6kV Switch Gear 계통 요건	확인단계			
		요건	설계	구현	시험
1	6.6kV 스위치 기어의 정상 전압을 OWS에 표시해야 한다.				
2	6.6kV 스위치 기어의 정상 전류를 OWS에 표시해야 한다.				
3	6.6kV 스위치 기어의 대체 전압을 OWS에 표시해야 한다.				
4	6.6kV 스위치 기어의 대체 전류를 OWS에 표시해야 한다.				
5	6.6kV 스위치 기어의 버스 전압을 OWS에 표시해야 한다.				

SDD(Software Design Description) transformed SRS into an architecture and a detailed design for each software component. In addition, the SDD V&V should demonstrate that the design is a correct, and accurate with a complete transformation of the SRS in which no unintended features are introduced.

In the software implementation, the system design is transformed into code, database structures, and related machine executable representations.

The test phase has two procedures: static and dynamic. To do dynamic test, we should have to ready a DTB_(dynamic test bed), which is made using a simulator enabling the reactivity of the reactor to be shown.

Thus, it is possible to verify the static and dynamic test of the logic.

The V&V of the test phase evaluated the completeness and consistency of the source code, as well as the test procedures and satisfaction of the performance requirements, based on traceability methods between the source code and the test procedure.

Finally, we verified the possibility to trace each step in accordance with the V&V through the performance of the SDLC.

4. Conclusions

This paper has discussed the software life-cycle V&V tasks for the control computer system in HANARO.

Tasks are composed of a total of 5 stages including software V&V plan and are used to analyze the traceability based on RTM_(Requirement Traceability Matrix) for verification of the design and manufacturing, regardless of the reflected requirements according to the IEEE 1012-2004 for the software verification.

Through this process, we implemented program without conversion and completed the testing of the functionality without any abnormalities.

I believe this process will be used in the design and manufacture of the HANARO in the future.

REFERENCES

[1] IEEE Standard for Software Verification and Validation 1012-2004
[2] KHCCS-VV101, Software V&V Plan & Procedure, 2013
[3] 이민우, 하나로 제어컴퓨터 교체 기술보고서, 2015
[4] Technical specification for programmable controller, TS-37-66400-001, KAERI/AECL, Daejeon, Korea, (1990)
[5] MW LEE, Replacement of HANARO Control Computer System, 2015.