Application of Software V&V Process for Instrumentation and Control System for Nuclear Power Plants

Dong Hee Kim[a], Sun Jin Byun[a], Yoon Hee Lee[a], Youngmi Kwon[b*]
[a] *I&C Dept., NSSS Division, KEPCO Engineering & Construction Company, Inc., Metropolitan Daejeon, Korea*
[b] *Dept. of Radio and Info. Comm. Eng., Chungnam National University, Korea*

[*] *Corresponding author: ymkwon@cnu.ac.kr*

1. Introduction

The software V&V (verification and validation) process used in Instrumentation and Control (I&C) system for Nuclear Power Plants is reviewed based on the Institute of Electrical and Electronic Engineers (IEEE) Standard 1012-2016 along with 2004. The software in nuclear power plants should be developed, tested, and qualified according to the regulatory guidelines and standards. Comprehensive processes for software V&V are introduced. In this paper, we studied the software V&V process specified in IEEE 1012-2004 and 2016, and reviewed detailed activities for their application in nuclear power plants. For software V&V area, there were no changes in terms of process and activities and between two standards. However, possible futuristic process and activities for project, system, and hardware are introduced in IEEE 1012-2016.

2. Overall Review and Results

In this section we review the overall process for software V&V specified in IEEE 1012. To meet the trend of regulatory environment in the domestic and foreign nuclear power plants, the establishment of optimized software V&V process is required. These new normal processes will be applicable to nuclear power plants in operation or under construction. And the optimized improvement in the process will be applied to the exported nuclear power plants.

2.1 Regulatory Guidelines for Software V&V Process

The regulatory position for software V&V process is provided in Regulatory Guide (RG) 1.168 [1]. This guideline endorses IEEE 1012-2004. The IEEE 1012, which is the typical standard document and revised in 2016, defines scope and activities for software V&V process. The IEEE 1012-2016 expands the scope of application from software V&V process to system, hardware, and software V&V process.

2.2 Definition of Software Integrity Level(SIL)

IEEE-1012-2004 classifies the Software Integrity Level(SIL) shown in Table 1 and defines minimum requirement for the Level 1~4 in system, hardware and software V&V process. Higher level requires more severe software V&V process. For example, the highest level (4) is classified as serious results such as loss of life, system failure, and economic and social damage.

Table 1 Software Integrity Level [2]

SIL	Effects/Damages following Failure
4	Catastrophic result/Loss of life, System loss, Economic and/or social loss, Impossible to recover
3	Serious results due to failure of system/ software (Eternal malfunction, Major system degradation, or social impact)/ Partial recovery or full recovery possible
2	Loss of partial functions generate problems. Full recovery possible
1	Loss of intended functions. Negligible impacts. Recovery unnecessary.

The SIL is determined on the agreement of stakeholders and its level can be changed during the lifetime of software.

2.3 Classification of the Software and Requirements

The software used for I&C system in Korean nuclear power plants is classified into 4 classes based upon its function and safety as follows; 1) Safety-Critical (SC) class used in safety system, 2) Important-to-safety (ITS), 3) Important-to-availability (ITA), 4) General Purpose (GP). Refer to Table 2 for definition of each class.

Table 2 Classification of the software

Class	Definition
SC	Initiation of reactor protection system, ECCS control signals
ITS	Control signal from Diverse Protection System, Monitoring and testing software for reactor protection system
ITA	Software for system and device used for plant operation
GP	General software that does not fall under the three levels

Software V&V process of SC class should comply with the requirements specified in Software Integrity Level (SIL) 4 of IEEE 1012 (Refer to Table 1). The ITS class should meet the requirement specified in Software

Integrity Level (SIL) 3. The software classified as ITA class should meet the requirement specified in Software Integrity Level (SIL) 2.

2.4 Software V&V Process

The V&V processes in IEEE Std. 1012-2004 and 2016 cover the 6 main processes as shown in Table 3. The process is defined as major six (6) steps of management, acquisition, supply, development (six activities in Table 3), operation, and maintenance.

Table 3 Six main processes of software V&V [2][3]

Process	**V&V Activity**	**V&V Task**
Management	Managing V&V Activities	Generate SVVP, Evaluate changes, Support review work
Acquisition	Acquisition support V&V	Defining scope of V&V
Supply	Plan V&V	Confirm contracts
Development	Concept V&V	Concept document review, Hazard analysis, Requirements assignment analysis, Traceability analysis
	Requirements V&V	Traceability analysis, Requirements evaluation, Interface analysis, Configuration management evaluation
	Design V&V	Traceability analysis, Design evaluation, V&V test design
	Implementation V&V	Traceability analysis, Source code evaluation, Component V&V, Perform test
	Test V&V	Traceability analysis, Acquire integrated system, Perform V&V test
	Installation and Checkout V&V	Audit installed system, V&V final report
Operation	Operation V&V	New constraint evaluation, Operation procedure evaluation
Maintenance	Maintenance V&V	Revise SVVP, Anomaly evaluation

2.5 V&V Activities per IEEE 1012-2016

New V&V activities that will be mandated for project, system, and hardware V&V process are;

Supply Planning V&V
Project Planning V&V
Configuration Management V&V

Design Definition V&V
System Analysis V&V

Hardware Integration V&V
Hardware Verification V&V

IEEE Std. 7-4.3.2-2016: "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations." is an IEEE standard that provides requirements and guidelines for designing digital devices (incl. FPGAs) used in safety systems for nuclear power plants. This standard plays a crucial role in ensuring the safety of nuclear power generating stations

2.6 Further Research

IEEE 1012-2016 provides an overview of V&V for projects, systems, and hardware tasks, and suggests that regulations will continue to be strengthened. Therefore, it is necessary to prepare for the strengthening trend of regulatory requirements in the future, including discussions and preparations for the roles of departments and organizations related to V&V tasks and DOR (Division of Responsibility).

3. Conclusion

The software verification and validation process used in Instrumentation and Control (I&C) system for Nuclear Power Plants is reviewed based on the Institute of Electrical and Electronic Engineers (IEEE) Standard 1012-2004 and 2016. It is required to optimize the Software V&V process following new overseas trend and new regulatory requirements studying guidelines and codes like 10 CFR 50 and IEEE 7-4.3.2. Therefore, further study on new codes like IEEE 1012-2016 and new strategies are required to implement changing requirements for system and hardware V&V in the future.

REFERENCES

[1] U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide (RG) 1.168, Revision 2, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 2013.

[2] Institute of Electrical and Electronic Engineers (IEEE) Std. 1012-2004, IEEE Standard for Software Verification and Validation.

[3] Institute of Electrical and Electronic Engineers (IEEE) Std. 1012-2016, IEEE Standard for Software Verification and Validation.

[4] IEEE Std. 7-4.3.2-2016: IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations.