Software Requirement Evaluation Method for Safety I&C System of Nuclear Power Plant

Jian-Zhong Tang(✉), Peng-Fei Gu, Sheng-Chao Wang, Ya-Nan He, and Wei-Hua Chen

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, Laboratory of I&C Equipment Qualification and Software V&V, China Nuclear Power Design CO., LTD, Shenzhen, China
tangjianzhong@cgnpc.com.cn

Abstract. Digital technology has been widely used in safety instrument and control (I&C) system of nuclear power plant (NPP). In order to guarantee high quality requirements about the safety I&C system of NPP, software Verification and Validation (V&V) should be implemented according to the standard IEEE 1012-2004. Software requirements evaluation would be done in different activities of software V&V. Even if the main tasks has been given in IEEE 1012-2004, the study about the evaluation methods is necessary to make progress in the implementation. Based on the practice about YangJiang units 5 and 6 projects, which is a Generation II+ pressurized water reactor, this study illustrates the software requirements evaluation methods of safety I&C system related to the laws and regulation standards. The system with evaluation indexes has been established which is also used in the practice of software V&V. Finally the effect has been analyzed from the process of V&V activities in the software development process. As a result, the analysis is also benefit to the design, development, operation and maintenance of safety I&C System as technical references in NPP.

Keywords: Safety I&C system · Software V&V
Documentation evaluation Index

1 Introduction

With the rapid construction of China's nuclear power project, and the promotion of the strategy of localization of nuclear power equipment as well as the "going out" with the nuclear power, the localization of safety digital control system (DCS), as the nerve center of the NPP, has also made a breakthrough. For example, the FirmSys, China's first nuclear safety instrumentation and control I&C system that was independently developed by Chinese Guangdong Nuclear Power Group Co. Ltd has been successfully launched and used in nuclear power project. NicSys8000N developed by CNNC Control Systems Engineering Ltd has also passed the independent engineering review of I&C systems [1]. As one of the necessary technologies to ensure the safety and reliability of the safety I&C systems in NPP, software V&V can effectively guarantee the software to meet the expected requirements of safety function and performance

Y. Xu et al. (eds.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 455,
https://doi.org/10.1007/978-981-10-7416-5_29

completely and correctly, that is to ensure that the software does not appear failure situation, and has received great attention in the field of nuclear power [2, 3]. In addition, it requires the I&C system products that implement safety functions in NPPs must conduct software V&V before launch [4].

The software V&V of digital safety I&C system for NPP runs through the whole process of software life cycle. It is used to conform that the activity output at each stage of the software life cycle can meet the requirements, and verify that the system can perform its expected function. The safety and reliability of software play an important role in ensuring system safety and avoiding heavy casualties and property losses so that there is an urgent need of the application of software safety and reliability analysis in the project [5]. While the independence, integrity and effectiveness of V&V activities are critical to ensure the safety and reliability of the safety digital control system software [6].

The software of safety I&C system in NPP is defined as the classification of safety according to the functional requirements [7]. The software V&V mainly refer to the requirements of IEEE 1012-2004, and perform the V&V tasks in accordance with the integrity Level 4 [8]. The activities of software V&V is divided into six major steps, namely: concept V&V, requirement V&V, design V&V, implementation V&V, integration test V&V, installation and checkout V&V. Because the requirement V&V is in the important position from software development outline design to detailed design, and considering the actual problem of huge amount of V&V activity input files, it is necessary to explore the activity of software requirements V&V, especially the V&V tasks included in the activity.

This article is organized as follows: the first part analyzes the content of the software requirements of safety I&C system of the NPP, combining with actual engineering to analyze the identification methods of software requirements, and proposes the software requirements evaluation method in the software requirements V&V; the second part analyzes the main indexes and key contents of the software requirement evaluation for the safety I&C system of NPP, and worked out the implementation steps for software requirements evaluation; the third part is combined with the software V&V activities of engineering practice, taking the practice of a nuclear power software V&V project as an example to illustrate the effectiveness of the software requirements evaluation method. At the same time, the challenges and directions of software requirements evaluation are summarized.

2 Software Requirement Identification of Safety I&C System in NPP

The software of safety I&C system in NPP is defined as the classification of safety according to the functional requirements. The software development process should meet the corresponding safety software requirements, and follow requirements of its product quality assurance system. According to the requirements of HAF 102-2004 and HAD 102/16-2004, for the safety digital I&C system software of NPP, the software V&V must be performed [9, 10].

According to the requirements of GB/T 13629-2008 and R.G. 1.168-2004, the safety I&C system NPP software should perform V&V in accordance with level 4 of integrity specified in IEEE 1012-2004 to check whether the software meets the requirements of relevant laws and regulations, user requirements and the requirements of I&C system of NPP [11, 12].

The software V&V NPP mainly includes six activities, namely: the concept V&V, the requirement V&V, the design V&V, the implementation V&V, the integration test V&V, the installation and checkout V&V.

The software concept V&V involves the design of system architecture and the analysis of system requirements, and puts forward the concrete solution to solve the users' problems, and the system architecture assigns the corresponding system requirements for hardware, software, and users' interface components. The software concept V&V activity verifies the correctness, accuracy and integrity of system requirements allocation, and make sure that the wrong assumptions are not entered into the program. The output of the software concept V&V activity, that is the system design transformed from system requirements assigned to the software, will be used as the input of software requirements V&V activity.

The software requirement V&V is to analyze the function and performance, the external interface of software, identification requirements, safety and security requirements, human engineering requirements, data definition requirements, the user documentation requirements of software, installation and acceptance requirements, user operations and implementation requirements, and user maintenance requirements, which is involved in the software of safety I&C system of NPP in order to ensure the correctness, integrity, accuracy, testability and consistency of software requirements.

The safety I&C system of NPP is a complex system engineering. For considerations of safety and reliability, the design and development of safety I&C system software in NPP requires to perform complex functional operations with simple program logic. Therefore, it is necessary to identify the software requirements before transforming the software requirements into detailed design and the subsequent code and the database structure. The relevant implementation standards, such as IEEE 1012-2004, only explicit that the software development should select the integrity level and complete the corresponding task according to function performed by the software, but there is no specific technical solution for the effective identification of software requirements. Through the engineering practice of CPR1000 nuclear power project, in order to identify software requirements effectively, it can be encircling the traceability analysis to make the inputs of software requirement V&V activity like requirements documents items and form the process records of software requirement analysis, providing the basis for subsequent analysis and evaluation of V&V tasks (Table 1).

Before the software requirements V&V starts the first is to clear the inputs of the activity, which is including the criterion documents and object documents. The criterion documents are the upstream input for software requirements V&V, that is the output of system concept design document of the concept V&V. While the object documents is the output software requirement analysis document of the requirements V&V. Through the item of requirement item for each input document of the software requirement V&V to perform the requirements of tasks. In the process of implementation of the V&V activity, if there is an anomaly in the input document, the opinion is

Table 1. Software requirements items

Number	Criterion document		Object document		Opinion	Record of anomaly item	Remarks
	Requirement items	Page number	Requirement items	Page number			
1							
2							
3							
……							

"to be discussed", corresponding to record the anomaly and organize the list, anomaly submitting them to the design and development parties for correction.

Through items of the requirement of input document of the software requirement V&V, it can effectively meet the requirements of V&V tasks, which is involving in huge amount of documents, drawings. And it also can identify the software requirements and discover the anomaly, ensure the safety and reliability of safety I&C system in NPP.

3 Software Requirement Evaluation of Safety I&C System in NPP

The software of safety I&C system in NPP is defined as the classification of safety according to the functional requirements NPP. The software requirement V&V need to be performed according to the integrity Level 4 in IEEE 1012-2004. The minimum task V&V involved in requirements V&V mainly includes: traceability analysis, software requirements evaluation, interface analysis, critical analysis, hazard analysis, risk analysis, safety analysis, configuration management evaluation, the generation of system test plan of verification and validation and acceptance test plan of verification and validation. In the software requirements identification of previous chapter, according to traceability analysis and interface analysis, document review and traceability analysis should be carried out firstly for requirement items. The result of identification and analysis of software requirements items can serve as a reference for software requirements evaluation and to evaluate the requirement document of software design and development phase combining with the index of software requirement evaluation.

The software requirement V&V undertakes the system design of the system requirements for the outline design software, and carries on detailed design and program implementation so that software requirements can be correctly identified. After the effective identification of software requirements, the identified software requirements and their analysis results should be evaluated. The purpose of the evaluation is assurance the correctness, consistency, completeness, accuracy, readability and testability of the software requirements. The corresponding evaluation indexes and their evaluation contents are shown in Table 2.

Evaluate the target content through the software requirements listed above, evaluate the requirements items that have been identified by entry division of software

Table 2. Software requirements evaluation indexes and contents

Number	Indexes	Evaluation content
1	Correctness	– Verify and confirm that the software requirements meet the requirements assigned to the software system under system assumptions, constraints, and operating environments; – Verify that software requirements meet the demand of standards, regulations, engineering references, regulations, policies, contracts and other documents; – Verify that data and control streams meet functional and performance requirements; – Confirm data usage and format.
2	Uniformity	– Verify that all the terms and their definitions are consistent; – Verify that the function can meet system requirements and procurement requirements; – Verify that each software requirement has internal consistency and has external consistency with system requirements.
3	Completeness	– Verify that the following elements are specified in the software requirements under system assumptions and constraints: • The software associative function (algorithms, status/mode definitions, input/output validation, exception handling, reports, logs, etc.); • Process definition and schedule; • The description of the hardware, software and user interface; • The performance criteria (such as: time requirements, size, capacity, speed, accuracy, precision, safety and prevention); • The control of system, device, and software (such as initialization, transaction and status monitoring, self-checking). – Verify that the software requirements meet the specified configuration management process.
4	Accuracy	– Verify that logic, computation, and interface accuracy (truncation and rounding) meet the requirements of the system environment; – Verify that the established physical model meets the requirements of system accuracy and natural laws.
5	Readability	– Make sure that the document is clear, understandable and unambiguous; – Verify all abbreviations, breviaries, terms, symbols that have been defined by the document.
6	Testability	– Verify the target acceptance criteria used to identify software requirements.

requirements. In the V&V project of nuclear power engineering software, refer to the exception grading principle of GJB2786A-2009, the identified abnormal items are divided into 5 grades according to the possible severity of the system failure consequences, namely “fatal”, “critical”, “important”, “general” and “suggestion” [13]. The requirement V&V can identify the existing abnormal items and risk items through the

process of identification, analysis and grading evaluation, the evaluation results can also provide reference for other V&V tasks, such as hazard risk analysis.

4 The Project Practice of Software V&V

Take the software V&V project of safety of instrument control system prototype of CPR1000 autonomous NPP as an example, using the software requirements identification and evaluation method proposed in this paper to evaluate the requirement of software in the requirement document so as to illustrate the effectiveness of the method. In document review and traceability analysis of requirements V&V, form 585 requirements check entries through the entry division of requirement document, 10 typical exception items are found, 1 of these is the "critical" issues in the software development process, the other 9 are the "important" issues that have not been reflected in the downstream software requirements document that from the upstream requirements of software in system design. Abnormal problems are summarized in Table 3.

Table 3. Software requirements items evaluation

Number	Exception summary	Exception influences	Grading evaluation
1	In the software requirements document, the technical content of the system design document is referenced directly and extensively. The software requirements document should be refinement and design solidification that based on the system design document, therefore, it is inconsistent with the design process	The lack of standardization of design process may lead to the subsequent development of software can't meet the relevant standards and regulations requirements, the user requirements and requirements of instrumentation control system of NPP	Critical
2	In the system design document, the related requirements of software can't be reflected in the software requirements document	Software requirements have not be identified and analyzed, which may lead to the loss of function or error implementation	Important

What needs to be explained is that, the implementation process and evaluation results described above are not only applicable to the requirements V&V in the software development life cycle, the other five verification and validation mentioned above are also apply. In this way, the whole process of software V&V development from requirement analysis, outline design, detailed design and transformation implementation to final integration test and installation test is formed. The entry analysis of software requirements is beneficial to keep the correctness, consistency, completeness and accuracy in the whole life cycle of software. If software development can be

considered from the began of whole life cycle, and achieve the best balance between development cost and the precision of software requirements entry, it will have a significant effect on the improvement of the quality of software.

5 Conclusion

Software requirement evaluation is one of the important V&V tasks of the requirement V&V in the whole life cycle of software development. Because it takes part the system architecture and requirements allocation for software outline design, and carry the detailed design and implementation of the software, in addition, the requirements V&V is in the field of the V&V project of nuclear power software. Therefore, the amount of input files involved has great practical challenges. How to evaluate software requirements efficiently is the key technology problem in the requirement V&V.

In this paper, by referring to the relevant requirements of the implementation standard of safety critical software of IEEE 1012-2004, combined with the engineering practice of V&V project of nuclear power software, summarize and refine the effective method of software requirement evaluation – the entry of software requirement. In the process of requirements V&V, according to the index content of software requirement evaluation, make grading evaluation of the requirement items in input documents, so as to get the design quality of software development from system design to the requirement analysis of software.

The software requirements evaluation method proposed in this paper can be applied to document requirement evaluation of all software V&V during the whole life cycle of software development, it can solve the problem of unclear or messy design of the documents requirement in the process of software development, which is beneficial to the abnormal traceability of the design and development, operation and maintenance of the safety of I&C system in NPPs, it also provides technical reference for the entry of software requirements and the traceability mapping of full life cycle in automation tools.

References

1. Ding, Y.X., Gu, P.F., et al.: Study on standard about safety digital I&C system in NPP. Process Autom. Instrum. **36**(11), 61–64 (2015)
2. Gu, P.F., Xi, W., Chen, W.H., et al.: Evaluation system of software concept V&V about the safety digital I&C system in nuclear power plant. In: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, vol. 400, pp. 125–132. Springer, Singapore (2016)
3. Liang, H.H., Gu, P.F., Tang, J.Z., et al.: A study of implementation V&V activities for safety software in the nuclear power plant. In: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, vol. 400, pp. 23–31. Springer, Singapore (2016)
4. Ye, W.P., Tang, J.Z., Chen, W.H.: Software V&V methods for safety digital I&C system of nuclear power plant. At. Energy Sci. Technol. **49**, 378–381 (2015)

5. Zhao, J., He, Y.-N., Gu, P.-F., et al.: Reliability of digital reactor protection system based on extenics. Springer Plus **5**(1), 1953 (2016)
6. Gu, P.F., Wang, S.C., Chen, W.H., et al.: A study about safety I&C system software V&V in nuclear power plant. In: The 24th International Conference on Nuclear Engineering, vol. 1, p. 005. American Society of Mechanical Engineers (2016)
7. International Electro Technical Commission: IEC 60880 Nuclear power plants-Instrumentation and control systems important to safety-Software aspects for computer-based systems performing category A functions. International Electro Technical Commission, Switzerland (2006)
8. Software Engineering Standards Committee of the IEEE Computer Society: IEEE 1012 IEEE Standard for Software Verification and Validation. Institute of Electrical and Electronics Engineer, New York (2004)
9. HAF 102: Safety of Nuclear Power Plant Design Regulations. Doctoral dissertation (2012)
10. HAD 102/16: Safety of Nuclear Power Plant Design Regulations Guides. Doctoral dissertation (2004)
11. GB/T 13629: Applicable standards for digital computer in safety system of nuclear power plant. Doctoral dissertation (2008)
12. R.G.1.168: Verification, validation, reviews, and audits for digital computer software used in safety systems of nuclear power plants. U.S Nuclear Regulatory Commission (2004)
13. GJB2786A: Military software General Development Requirement. Doctoral dissertation (2009)