Evaluation System of Software Concept V&V About the Safety Digital I&C System in Nuclear Power Plant

Peng-Fei Gu, Wang Xi, Wei-Hua Chen and Su-Yuan Yu

Abstract Since the digital technology was used in the safety digital I&C (Instrument and Control) system of nuclear power plant (NPP), its safety and reliability have been one of the most important factors to the safety operation of NPP. V&V activity is a significant method to insure the safety and reliability of the nuclear power I&C system software, the system to evaluate the efficient of V&V activity need further research. This paper on the basis of CPR1000 NPP Reactor Protection System (RPS) software development project, use the concept V&V activity for example, make a discussion for the evaluation of V&V activity, including the description of general tasks, definition of the Failure Modes, and analysis of V&V activity by FMEA (Failure Modes Effects Analysis). The results of our evaluation method in project show that the efficiency of V&V activities has been improved, and provide references for the evaluation to other NPP I&C system software development V&V activity.

Keywords Nuclear power plant · I&C · V&V · FMEA

1 Introduction

As the active development strategies for nuclear power, the installed capacity of which will reach 70–100 GWe at the time of 2020, account for more than 4% of the total installed capacity in China, and the proportion should be at least added to 6%

P.-F. Gu (✉) · S.-Y. Yu
Institute of Nuclear and New Energy Technology, Collaborative Innovation Center of Advanced Nuclear Energy Technology, Tsinghua University, Beijing, China
e-mail: gupengfei@cgnpc.com.cn

P.-F. Gu · W. Xi · W.-H. Chen
Instrumentation and Control Department, China Nuclear Power Design Co., Ltd., Shenzhen, China
e-mail: wang.xi2@cgnpc.com.cn

W.-H. Chen
e-mail: chenweihua@cgnpc.com.cn

Y. Xu (ed.), *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, Lecture Notes in Electrical Engineering 400,
DOI 10.1007/978-981-10-3361-2_14

according to the Low Carbon (LC) plan with the installed capacity arriving at 150–200 GWe in the year of 2030. The time limit for a complement construction of NPP is more than 5 years, which means there are 10 nuclear power units for each year from now to the year of 2025. A mature, quantity production stage for the development of nuclear power is coming for us.

The sustainable development of nuclear power station not only relies on the acceptance of the nuclear economy in public, the improvement of the safety and reliability in nuclear technology is also more significant. The nuclear Digital Control System (DCS) is one of the most important devices for the safety of nuclear power station. Software is the kernel of DCS, which on the basis of CPU, to achieve the protection and logic of the devices for nuclear power station. The safety of the software affects the safety, reliability and economy of the NPP directly. Therefore, a strict verification and validation (V&V) activity for the whole lifecycle of software development is necessary [1, 2], and the method to evaluate the effectiveness of the V&V activity should be further discussion.

This paper arranged as follow. Section 2 introduces the work of V&V activity for DCS software development in NPP, and propose the general tasks and key points for the evaluate of concept V&V; Sect. 3 makes definitions for failure modes including the general tasks and key points; Sect. 4 combines to the CPR1000 project, bases on the constructed failure modes, use FMEA method to analyze and improve the V&V activity; Sect. 5 make a conclusion for the whole paper.

2 V&V Activities and Tasks

V&V activity is an important method to assure the quality of software. Verification conforms to requirements for all activities during each life cycle process, satisfies the standards, practices, and conventions during lifecycle processes. Validation satisfies system requirements allocated to the products at the end lifecycle activity, solves the right problem, and satisfies intended use and user needs in the operational environment [3]. V&V activity aims to locate and recognize the default or errors in the software, assure the correct process of software development, make the products satisfy the whole requirements from user, and assure the consistency of computer software and the technology requirements, make sure of the software functions correctly in the environment designed previously [4].

2.1 V&V General Tasks

According to HAD 102/16 (2004) [5], IEEE1012-2004 and IEC60880 [6], the V&V activities for DCS in NPP process by 6 stages, including management process, acquisition process, supply process, development process, operation process, and maintenance process. The most significant stage among them is the

development process, in which the main V&V activities including Concept V&V, Requirements V&V, Design V&V, Implementation V&V, Integration test V&V, Installation V&V and checkout V&V. For each V&V activity, there are tasks to be complemented, named general tasks.

This paper use concept V&V as example to introduce the general tasks.

2.1.1 Concept Documentation Evaluation

Concept documentation evaluation insures that the concept documentation satisfies use requirements and complies with the precede needs, assures the restrains of interfacing systems and the imposed restrictions on provided approach, make analysis on system requirement and ensure the needs from user, including system function, end-to-end system performance, operation and maintenance requirements and so on.

2.1.2 Traceability Analysis

The traceability analysis implemented as follow. Firstly, make identification for the whole system needs, which should be accomplished completely or partially by software. Then, verify that precede needs can be traced by the system requirements. Finally, the traceability analysis starts between the software requirements and system requirements.

2.1.3 Requirements Allocation Analysis on Hardware, Software and User

The analysis verifies the completeness, correctness and accuracy of the concept requirement that has been allocated to hardware, software, and user interfaces for user needs. The completeness verifies that user needs should be satisfied by follows, including failure detection, isolation, diagnostic, and error recovery. The correctness verifies hardware, software, and user interfaces have been allocated to those performance requirements that satisfy the needs from user. The accuracy including the verification of the specification of external and internal interfaces for interface protocols, data formats, and the frequency of data exchange.

2.1.4 Hazard Analysis

Hazard analysis analyzes the potential dangerous to and from the concept system, including the identification of the potential system hazards and mitigation strategies for each hazard, the accession of the severity and the probability of each hazard.

2.1.5 Risk Analysis

The risk analysis including two parts, the identification of the technical and management risk, the proposed suggestions to mitigate or decrease the risks.

2.1.6 Security Analysis

The security analysis including: review the acceptable level of security, and then ensure confidentiality, integrity, availability, and accountability. Surely the risk related to system interfaces should be analyzed.

2.1.7 Criticality Analysis

The main activities of criticality analysis pay attention to the integrity levels [7], make sure that software integrity levels have been established for detailed functions, software modules, requirements, subsystem, or other software partitions; make verification of the assigned software integrity levels to be correct; insure the software integrity levels have been assigned to individual software components. The assignment of the software system should be the same as highest level assigned to any individual element; the assignment of software component should be the same or higher than the software integrity level, while any software component that can influence individual software components are assigned a higher software integrity level.

2.2 V&V Key Points

The concept V&V activities should pay more attention to the "key points", which reflect a specific consideration for the nuclear power station engineering project. An evaluation of whether these "key points" has been considered in software V&V activity could show further effectiveness of V&V works. This paper discusses the importance of DCS Contracts and the Requirement Tracing on the basis of the V&V activity in CPR1000 RPS DCS software development project.

2.2.1 DCS Contracts

The DCS contracts should be included in the input documents as the reference files that can be traced.

Theoretically, the RPS specification is the baseline of concept V&V activities. With the progressively implementation of the construction of NPP, the technical details in DCS contracts, which signed at the beginning of engineering project for

the consideration of the whole schedule, may not in consistent with the RPS specification, these inconsistent points cannot satisfy the original requirements of the NPP. Therefore the analysis of technical points is necessary.

2.2.2 Requirement Tracing

As the part of the requirement management [8], the requirement tracing establish traceability links [9] between every neighboring stages to provide a foundation for requirement modification management and version control. As the NPP DCS RPS software lifecycle has covered each stage including development, operation, and maintenance and so on, the mistakes and errors discovered in V&V activity not only beneficial to the quality assurance, and also provide a convenient for the Experience feedback of succession operation and maintenance if the NPP need renovation. Therefore, the requirement tracing matrix should be established exactly at the beginning of concept V&V.

3 Definitions of Failure Modes

Failure modes means the system or its sub-system or components do not satisfy their design or function of system requirements, as the example of the concept V&V illustrated in Table 1, Failure modes can be classified into five parts, including the inconsistent of legislation and standards, Lack of general tasks, Unaccomplished plan, inconsideration of the specific in engineering project, and Uncompleted requirement tracing. The definitions can be used for the classification of the Failures events that discovered by V&V activity.

Table 1 Definitions of failure modes in concept V&V activity

V&V activities	Failure modes	Definitions
Concept V&V	Inconsistent of legislation and standards	The V&V tasks are not in consistent of legislations and standards such as HAD102, IEEE1012
	Lack of general tasks	Lack of general tasks, such as hazards analysis
	Unaccomplished plan	The formulated plans for V&V activities haven't been totally accomplished
	Inconsideration of the specific in engineering project	The DCS contracts are not included in input documents
	Uncompleted requirement tracing	The requirements are not arranged to entries and tracked by using a requirement tracing tool

4 Failure Modes and Effect Analysis

The project, of which this paper on the basis, uses FMEA (Failure Mode and Effect Analysis) method to do an effectiveness analysis for concept V&V activities. In this project, according to the FMEA result for the first round concept V&V activity and the project schedule, the V&V teams formulate improvement measures for the second round concept V&V activity, and according to the FMEA result for the second round concept V&V activity and the project schedule, V&V teams formulate improvement measures for the third round concept V&V activity.

The FMEA results of the concept V&V activity in the project are described in Table 2, the "Failure results" means an uncompleted tasks results in V&V for the reason of the corresponding "Failure Modes"; The "Effect Analysis" evaluates the influence on the effectiveness of V&V activities by analyzing the failure events; "Improvements" assure the effectiveness of V&V activities by formulating improved method; "Problem Classifications" illustrated in Table 3, which defines the different levels of problems according to influences on V&V activity.

As showed in Table 3, to solve the failure modes, the backward tracing is done in the second round concept V&V activity; The requirement tracing tool named DOORS [10] is used in the second round concept V&V activity to establish the requirement tracing matrix; The FMEA method is used in the second round concept V&V activity and product the reports for the hazard analysis; The DCS contracts are included in the foundation documents for analysis in the third round concept V&V activity. Compared to the first round, the second round concept V&V activity discovered other 51 mistakes or errors, and the third round concept V&V activity find other 34 questions, by use the FMECA (Failure Mode Effect and Criticality Analysis) [11] method, an enhanced effectiveness of V&V activity has been showed in project results.

Table 2 Problem classifications

Problem levels	Discretions
Serious	Events will lead to the failure of the whole V&V activities.
Important	Events will result in losing of important contents of V&V activities
General	Partly influence on V&V activities and need pay further attention to the analysis of effectiveness for V&V activities
Suggestion	No influence on the effectiveness of V&V activities, but may lead to unfavorable operations and maintenances in the future

Table 3 FMEA results of concept V&V activities

No.	Failure modes	Failure results	Effect analysis	Improvements	Problem classifications
1	Lack of general tasks	The backward tracing is not done in the first round concept V&V activity	Ignoring of the extra requirements in DCS design file, and result in the failure of V&V activities that extra functions have been designed in system	The backward tracing is done in the second round concept V&V activity	Serious
2	Uncompleted requirement tracing	The requirement tracing is not done in the first round concept V&V activity	It is difficult to implement the requirement tracing in the succession V&V activities	The requirement tracing tool named DOORS is used in the second round concept V&V activity to establish the requirement tracing matrix	Suggestion
3	Unaccomplished plan	The hazards analysis, which is formulated in the plan, is not done in the first round concept V&V activity	The mistakes and errors cannot be found in system structures and the safety of functions cannot be analyzed	The FMECA method is used in the second round concept V&V activity	Important
4	Inconsideration of the specific in engineering project	The DCS contracts are not included and analyzed in the foundation documents in the second round concept V&V activity	The technical details in the DCS contracts that inconsistent with the RPS specification may not be found and result in lack of analysis for the differences	The DCS contracts are included in the foundation documents for analysis in the third round concept V&V activity	Important

5 Conclusions

On the basis of CPR1000 NPP RPS software development project, this paper gives a further discussion for V&V evaluation system, use FMEA system method to analyze the failure modes and results in V&V activities and provide improvements. By using the improvements in succession V&V activities, an enhanced efficiency of V&V activity has been showed in results of project, provides an reference for the evaluation of other NPP I&C software V&V activities.

Acknowledgements This project was financially supported with funds which provided by a reliability research of reactor protection system which based on digital microprocessor and electrical equipment (national science and technology major project). The award number is 2014ZX06004002-004.

References

1. Liu Z, Jiang G J, Sun Y B (2011) The V&V activities and techniques for safety-class I&C system in the nuclear power plant [J]. Chinese Journal of Nuclear Science and Engineering, 31(2):45–50.
2. Software Engineering Standards Committee of the IEEE Computer Society (2004) IEEE 1012 IEEE Standard for Software Verification and Validation [S]. Institute of Electrical and Electronics Engineer, New York.
3. R.G. 1.152 (2006) CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS [S]. U.S NUCLEAR REGULATORY COMMISSION.
4. International Electro technical Commission (2006) IEC 60880 Nuclear power plants-Instrumentation and control systems important to safety-Software aspects for computer-based systems performing category a functions [S]. International Electro technical Commission, Switzerland.
5. HAD 102/16 (2004) Safety of Nuclear Power Plant Design Regulations Guides [S]. Doctoral dissertation.
6. Nuclear Power Engineering Committee of the IEEE Power Engineering Committee (2010) IEEE 7-4.3.2 IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations [S]. Institute of Electrical and Electronics Engineers, New York.
7. Ding Y X, Gu P F, et al. (2015) Study on Standard about Safety Digital I&C System in NPP [J]. PROCESS AUTOMATION INSTRUMENTATION, 36(11):61–64.
8. Xia D Y, LIU W P (2015) Requirement Management on Nuclear Power Plant DCS for Development [J]. INSTRUMENTATION, 22(2):63–66.
9. Xiao W (2012) An Optimized Method for Software Requirement Development Process Using Doors [J]. Computer Application and Software, 29(9):175–177.
10. IBM Corporation (2010) Rational DOORS Help [CP/DK], IBM Corporation.
11. Wu X K, Wang G S (2014) Nuclear Safety Digital I&C System Software V&V Technical Standards Research [J]. Nuclear Standard Measurement and Quality, (4):16–22.