A Study of Implementation V&V Activities for Safety Software in the Nuclear Power Plant

Hui-hui Liang, Peng-fei Gu, Jian-zhong Tang and Wei-hua Chen

Abstract In order to improve the safety and reliability of the safety related software for the nuclear power plant, the verification and validation (V&V) is necessary for the software in the whole development life cycle based on nuclear laws and principles requirement. Nuclear Safety software implementation phase means using programming language to perform system requirement specifications. Implementation V&V activities based software design documentation to verification and validation the correctness, accuracy and completeness of the source code. This paper considered the regulation and law requirements and given the test types of implementation V&V activities. The test process of implementation V&V activities for safety software in nuclear power plant has been given. The paper also proposed the key points of the test case and the principles that the test person need to follow.

Keywords Safety software · Implementation V&V activities · Test type · Execute

1 Introduction

The safety and reliability of nuclear safety application software will directly affect the entire nuclear power plant safety and economy. To ensure the quality level and improve nuclear safety level of reliability, nuclear safety application software need to perform independent software verification and validation (V&V) work within the entire development life cycle. Nuclear power plant safety applications software V&V work is the key point to self-developed nuclear safety-class system.

H. Liang (✉) · P. Gu · J. Tang · W. Chen
State Key Laboratory of Nuclear Power Safety Monitoring Technology
and Equipment, China Nuclear Power Design CO., LTD, Shenzhen, China
e-mail: lianghuihui@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_3

According to IEEE 1012 [1], software V&V activities include concept V&V, requirement V&V, design V&V, implementation V&V and integration V&V and so on. The software implementation phase means using programming language to perform system requirement specifications. The implementation phase will generate the source code that the computer can read. Implementation V&V activities are based on software design documentation to verification and validation the source code is correctness, accuracy and completeness.

The V&V standards and regulations are developed by the international organizations, such as IEEE [1, 2], NRC [3] and IEC [4]. The domestic [5–7] is also to compile the standards and guidance documents. The standards and regulations only give the software V&V activities and performance requirements. They don't carry out the system implementation process and what test type need to be executed for the software implementation phase V&V.

The paper is organized as follows. The first part introduced the research background. The second part collates the domestic and international standards and regulations for the safety application software V&V test. The second part gives the test types that need to be performed in the safety application software implementation V&V. The third part presents the implementation phase V&V test process and methods which considers the test type. The fourth part is the conclusion.

2 Software Test Requirements in Regulations and Standards

In order to achieve the better results of nuclear power plant safety software V&V activities, the nuclear advanced countries build the nuclear power plant V&V regulations and standards. The International Atomic Energy Agency (IAEA) and International Electro technical Commission (IEC) promulgate the nuclear power plant software V&V standards and regulations. IEC 60880 [4] gives the rules of design and documentation for the category A functions software. It includes specification, design, verification and validation, etc. IEEE 1012 [1] is the verification and validation standard for system and software. It regulates the content, scope, method and demand of the software implementation V&V activities. It also gives the minimum task set. IEEE 1028 [8] describes the guidance on how to conduct software reviews, inspections, technical and management review. It provides the reference for the implementation V&V activities. IEEE 829 [9] gives the purpose, content, formal and key elements of software test. The NRC R.G.1.170 [10] accepts IEEE 829. The software unit test requirements and method is put forward by IEEE 1008 [11] and R.G.1.171 [12]. The domestic standards and regulations are mostly transformed by IEC. HAD 102/16 [5] provides the verification and validation plan.

Based on NB/T 20054-2011 [7], the nuclear plant A category function software should be divided into module when the program is designed. So the implementation V&V activities for safety-class software need to test the module units before component test.

3 Test Types for Implementation V&V Activities

The application software implementation V&V activities include the module unit, function, interface and component test. The unit test is to verify the software units satisfy the software specifications and coding standards. Currently the test types for high security application include dozens. The paper combines the nuclear safety software its own characteristics and standard and regulation requirements that gives the test types in the software implementation V&V activities.

The standard and regulation requirements provide the following demands for the software and documents:

1. The software satisfies the software specification and it can be verified. The code can also be read, understood and has adequate comments.
2. The code should be simple. The recursive structure, code compression and optimization need to be avoided.
3. The data structure and name should be consistent in the whole system. It includes data type, scope, accuracy and so on.
4. In order to regulate and guide the program design, the approved encoding rules are requisite.
5. The software should be testability that means the every executable code can be interviewed.
6. The document should include software design specification and logical requirements. It also needs to contain pre-condition and post-condition for every module.
7. The input and output variable, the effective scope and interface should be described in the document.
8. The document and software should give the methods of abnormal situation. The reliability and safety measures are also needed to consider.

Due to the aforementioned conditions, the nuclear safety application software implementation V&V need to performed the minimum set of the test type as shown in Table 1. From Table 1, we can see that the nuclear safety application software implementation V&V need to execute at least thirteen test types.

Table 1 Test types of implementation V&V activities for safety application software in the nuclear power plant

No.	Test type	Requirement specification
1	Document review	Do completeness, consistency, accuracy and correctness review for requirement documents
2	Code review	Review the code consistent with requirement documents and standards and code structure design is reasonable and code readability
3	Static analysis	It includes data flow analysis, control flow analysis, and information flow analysis
4	Code walkthrough	Code walkthrough is a way of checking the code design flaw. Code walkthrough executes the test case by human brain to verify the code to run properly and meet the functional requirements
5	Logical test	Logical test is to verify the software logical structure is correct. It is able to achieve all branch and statement coverage and make sure that the code does not exist any infinite loops or redundant branches or statements
6	Function test	Functional test needs to verify every functional requirement. Functional test needs to verify the normal and abnormal situation for every module
7	Interface test	Interface test should perform the conformance between the software interface data types and structures. Input and output interfaces for each module should be executed the abnormal and normal test
8	Reliability test	The specific test need to be performed for the situation which may change the operation mode. It includes the boundary and environmental test. The human negligence design which will affect the software reliability that should be avoided, such as division by zero
9	Regulatory compliance test	The compliance between the application software design and the development standards should be executed. Standards compliance evaluation criteria should be established
10	Compatibility test	Nuclear safety application software compatibility test mainly refers to the new version application software to retain the old version function. In this case, it needs to verify the compatibility between the two versions, the potential risks and incompatibilities
11	Performance test	Nuclear safety application software implementation V&V performance test is mainly for the response time, accuracy of the output data and other critical functions
12	Boundary test	Boundary test is the running state test when the software in the boundary and endpoint. It includes state transition boundary, functional boundary and properties boundary
13	Data processing test	Data processing test includes the conversion of test data, test data acquisition and the capability of removing the bad data

4 Implementation V&V Activities

Nuclear Safety software implementation V&V test technology and methods can be divided into static test and dynamic test. The nuclear safety software implementation V&V test can be divided into document review, code walkthrough and code analysis, unit test and component test.

1. Document review

It is mainly to review the software module unit document in the correctness, completeness, accuracy, consistency. The tester need to verification and validation the demands of software module unit documentation are traceable.

2. Code walkthrough and code analysis

Code walkthrough and code analysis is static test. Static test is not running the program. It executes the program and document analysis and examination. The analysis can use the automation tools which have been reviewed by the project in order to improve the efficiency and quality assurance.

Code walkthrough and code analysis focus on the following problems:

- The document describes inconsistent;
- Code is inconsistent with the requirements document;
- The compliance between code implementation process and the standard;
- Code structure problem;
- Code protection mechanism.

3. Unit test and component test

Unit test and component test is dynamic test. Dynamic test runs the program and achieves the software errors and defects by executing a set of instance data. Software coverage index is a common way to assess the adequacy of the dynamic test. The design of nuclear safety application software test case should consider statement coverage, branch coverage and MC/DC coverage.

In order to find as many as the program design flaws, perfect test case is essential. Table 2 is the compared result which is the different team executes the same project. The project is to test the function for the ordering system. Team A fund thirty one problems by implementing five hundred two test cases. But team B just executed three hundred forty three test cases and fund thirty three problems. So the reasonable and effective case will cover various types of test requirements and coverage metrics, reduce test effort and efficiency work.

Table 2 Compared team A with team B in the same project

Number	Team A	Team B
Test cases	502	343
Problems	31	33

Nuclear Safety software implementation phase V&V test case design needs to be completed after the software requirements specification has been finished. The following key factors should consider when the nuclear safety software implementation V&V design the test case.

- The normal and abnormal value design;
- Each test case needs as many contain multiple test types;
- It need to give a reasonable and feasible evaluation criteria for each test case;
- A test case needs to consider the effective equivalence class;
- The test cases need to cover every requirement;
- The test cases preferably prepared by the engineers which have the relevant project experience.

Unit test and component test include the following common problems.

- Functional description is inconsistent with the requirement;
- Data processing exists risk, such as data accuracy;
- Abnormal value or boundaries don't give the protection mechanisms;
- Interface inconsistencies.

5 Quality Assurance

Nuclear Safety software implementation V&V need to write the test plan and instruction. The test plan includes personnel, scope, purpose, schedule, exception handling quality assurance programs. Test instruction used to guide and regulate the implementation of test cases. The tester should ensure completely and correctly execute the test cases. Tester should comply with the following requirements.

- Testers need to organize test procedures, test plan and test management training files before performing the test;
- Test cases need to be completely and accurately execute in step;
- Testers need to record the real test environment and test results to ensure test repeatability;
- Adding or changing the test case need to be confirmed by the technical director.

6 Application

Above implementation V&V activities for safety-class application in the nuclear power plant had been applied to the CPR1000 project. The project involved nearly two hundred thousand code lines and included four versions. The code lines existed small changes because of the software modules increasing and revising. Problem statistics shows in Figs. 1, 2, 3 and 4. The problems of four versions software were one-hundred-three, sixty-six, twenty-six and nineteen as show in Fig. 5.

Fig. 1 The first vision software problem statistics

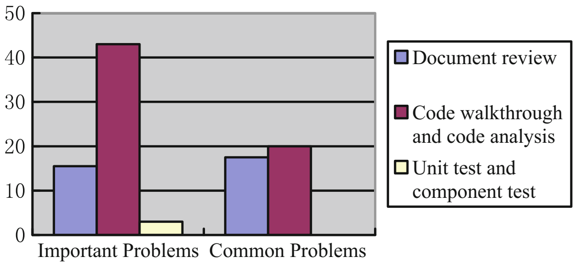


Fig. 2 The second vision software problem statistics

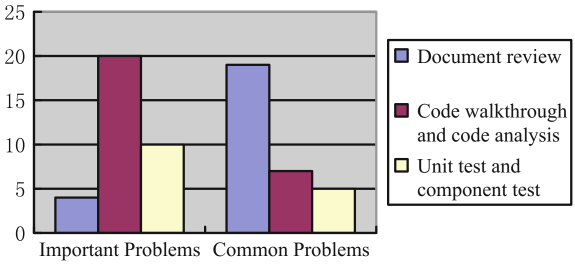


Fig. 3 The third vision software problem statistics

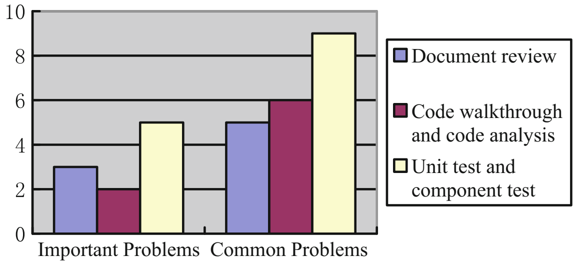
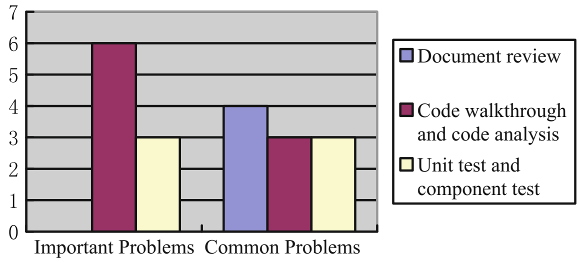
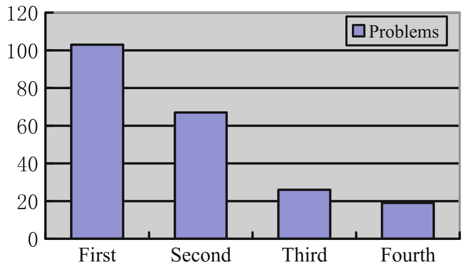


Fig. 4 The fourth vision software problem statistics



From Fig. 1, the problems were focus on software implementation. The test team found sixty-seven problems through code walkthrough and code analysis. The main problems were the process of the documentation requirements transformed into software. Through the three visions testing, the third and fourth visions software problems concentrated on the documentation requirements. That means the

Fig. 5 Problem statistics of four visions



imperfect demands lead to the software problems. As shown in the Fig. 5, the problems are gradually reduce. The implementation V&V activities improved the reliability and safety for the safety-class application in the nuclear power plant.

7 Conclusion

This article had analyzed and discussed the test types for the nuclear safety applications software implementation V&V activities. The paper proposed the minimum test type set for the nuclear safety application software implementation V&V activities. The paper also described how to execute the implementation V&V activities. In order to ensure quality, the paper given the key factor what the person need to obey. Through the actual project verified the effectiveness of implementation V&V activities. It provided a reference and guidance for nuclear safety software implementation 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. IEEE 1012 (2004). IEEE Standard for Software Verification and Validation.
2. IEEE 7-4.3.2 (2010). IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.
3. R.G.1.168 (2013). Verification, Validation, Reviews and Audits for Digital Computer Software Used in safety Systems of Nuclear Power Plant.
4. IEC 60880 (2006). Nuclear Power Plants Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions.
5. HAD 102/16 (2004). Systems Important to Safety Based on Computer of Nuclear Power Plants.
6. HAF102 (2004). Regulate for Nuclear Power Plant Design Safety.

7. NB/T 20054 (2011). Nuclear Power Plants Instrumentation and Control System Important to Safety Software Aspects for Computer based System Performing Category A Functions.
8. IEEE 1028 (1997). IEEE Standard for Software Reviews.
9. IEEE 829 (1998). IEEE Standard for Software Test Documentation.
10. R.G.1.170 (1997). Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants.
11. IEEE 1008 (1987). IEEE Standard for Software Unit Test.
12. R.G.1.171 (1997). Software Unit Test for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.