Research and Application of the Verification and Validation Method Based on Embedded Technology in Nuclear Power Plants

Chao Zhang(✉), Wang-Ping Ye, Sheng-Chao Wang, and Ji Shi

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, China

Abstract. This paper introduces a new method of research and application of software V&V based on embedded technology in Nuclear Power Plants. Based on software abstract test, the relationship between defect trend and cost is analyzed. Mind map test analysis is carried out, and the V&V levels are carefully defined and divided. System tests based on model are carried out. Specification-based tests and code-based unit-level tests are organically combined. Finally, this paper summarizes the V&V scheme. This V&V method based on embedded technology has been unanimously approved by experts and has a widely application prospect.

Keywords: Embedded technology · V&V · Nuclear power plant · Mind map

1 Introduction

With the continuous development and application of the three generations of nuclear power technology, embedded system architecture, as the computerized system of microprocessor technology, is frequently applied in security important systems. In order to ensure the security and reliability objectives, embedded software testing plays an important role. In order to discover software defects, repair software defects and software quality ultimately improve. The failure of embedded system security may lead to disastrous consequences. Especially, the failure of security will lead to significant risks and economic losses in nuclear safety-related systems. Embedded software V&V requires higher reliability than ordinary software. This requires strictly testing, verification and validation of embedded software to improve the reliability of products. When embedded systems/equipment are used to implement safety function, they need to meet the regulatory requirements of the regulatory authority, as well as the appraisal requirements of the owners and purchasers.

Some traditional testing methods couldn't satisfy the rapid development of software testing industry. New testing methods are proposed to make up for the deficiencies of the existing software testing, such as "embedded testing design based on business scenarios", "embedded testing design based on risks", "embedded testing design based on task-driven" and "embedded testing design based on exploration". Due to the increasing

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 463–469, 2021.
https://doi.org/10.1007/978-981-16-3456-7_45

complexity and functions of the software, manual testing couldn't meet the fast iteration. In order to solve this problem, automated tools need to be used instead of complex testing processes. In terms of hardware qualification, there is a full set of mature qualification methods to ensure its reliability, such as seismic qualification and electromagnetic compatibility qualification [6].

The main contents of this research include the relevant laws and standards of embedded software V&V for important nuclear safety systems. This paper establishes an embedded software V&V technical scheme and method suitable for safety important systems in NPP. The application effect of the scheme and method tests in project practice. This paper summarizes the technical key points in the embedded software V&V process of safety important systems in NPP.

2 Research on Standards

The premise of embedded software V&V is meeting the regulations and standards. Different software testing stages require different regulations and standards for embedded software V&V activities and tasks. The standard conformity analysis is carried out in combination with the work of each stage. The International Atomic Energy Agency (IAEA) and the International Electronic Technical Commission (IEC) promulgate the nuclear power plant Software V&V standards and regulations. IEC 61508-3 defines the functional safety of electronic/electronic/programmable electronic safety-related systems [1]. It specifies the independence of software development, and performs appropriate common cause failure analysis. When credible failure mechanisms are identified, effective defense measures should be taken. The correctness of embedded software is ensured from five dimensions: Safety Function, system configuration, Hardware security integrity requirements, Software system capability requirements, capacity and response time. IEC 62138 specifies the requirements for nuclear power plants instrumentation and control important for safety Software aspects for computer-based systems performing category B and C functions. It is applicable to each stage of the nuclear power plant life cycle of software computer-based systems [2].

IEEE 1012 defines the V&V process in terms of specific activities and related tasks, and also defines the V&V plan [3]. Software V&V runs through the whole life cycle of the product process, such as evaluation, analysis, evaluation, review, review and testing. V&V process includes verification process and validation process.

3 V&V Scheme

The V&V scheme decomposes and concretizes the test contents. The test is more and more feasible and intuitive, and the test process is easier to understand. The test scheme plays a very good guiding and leading role in the compilation of test cases, the construction of test environment and the implementation and execution of tests.

Software test is an important research field in software project. It is also one of the purposes of verification and validation software tests, which is to find defects as much as possible. From another perspective, software test would help people to have a deeper

understanding of the differences between software actual behavior and expected behavior. In order to fully carry out the software test, it is required to make a complete analysis of software input/output space. Software test abstraction is shown in Fig. 1. Its basic composition includes software S, test specification R and software input/output space. Software expected output behavior could be obtained according to the test specification R, while software real output behavior could only be obtained according to the actual operation of software.

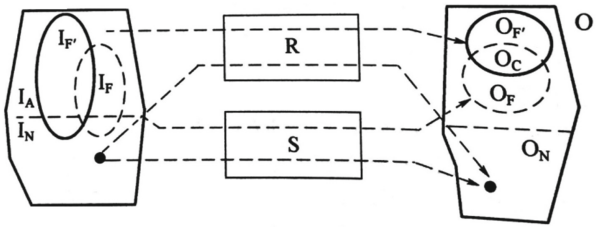

Fig. 1. Software test abstraction

On the foundation of research and standard research, the V&V team has formed the embedded software V&V general scheme shown in Fig. 2. "Development and Application of Computer Software Based on Embedded Technology Safety Analysis in Nuclear Power Plants" divides the qualification activities of safety analysis software into phases including concept V&V, requirement V&V, design V&V, implement V&V and test V&V

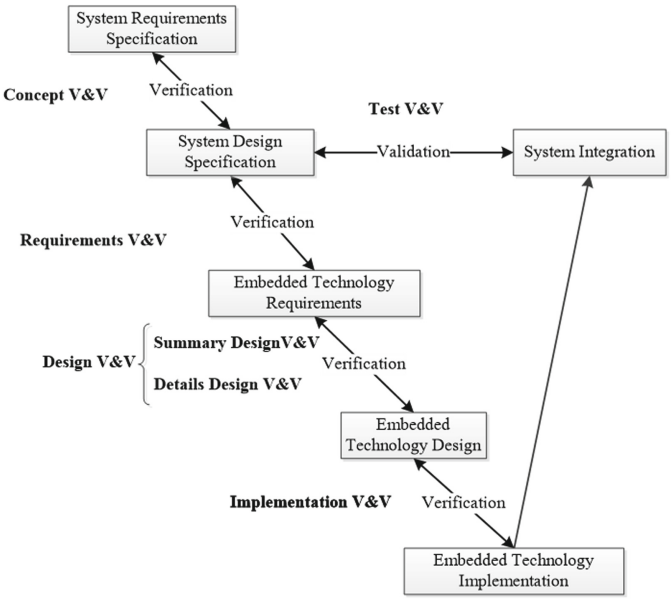

Fig. 2. General scheme of embedded technology V&V in nuclear power plant

[7, 8]. This scheme covers all test requirements. It is testable and executed. It has been reviewed and approved by relevant project testers, research and development personnel, product managers and experts. This scheme could provide reference for the design of research and development products. It could improve the understanding of the requirements of the project team members and at the same time strengthen the recognition of the testing work. In the end, it enhances trust in test quality and results.

4 V&V Strategy

The V&V strategy includes both tested and untested features. According to the test item description, the tester determines the specific test focus and strategy, as shown in Table 1. It includes the product functions of the test, the key points of the test and the corresponding test technologies and methods. In the end, it provides evidence for writing test cases.

Table 1. Functional tests

Serial number	Product function description	Test focus	Testing techniques and methods	Comments
1	… …	… …	… …	\
2	… …	… …	… …	\

According to the test plan, the test function items are divided. The test points are extracted from the test items, including the function points, performance, safety, stability, compatibility, ease of use, etc. The second and third levels of test analysis using mind

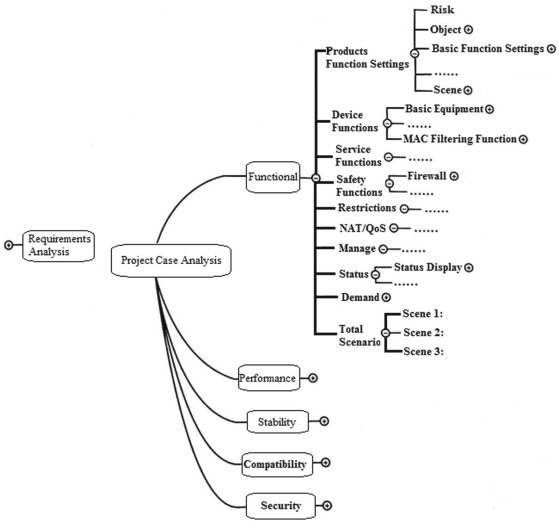

Fig. 3. Mind map test analysis

maps can correspond to the description of test items in the scheme. Since the mind map is produced earlier than the test plan, the tester would well determine the test range and function items according to the mind map. The analysis of mind map test is shown in Fig. 3.

5 V&V Activities and Tasks

According to the requirements of performing Class B functions, the scheme matches IEEE 1012 activities and tasks. It summarizes the specific tasks and common tasks of the five major stages in Table 2. The V&V work plan report should be compiled and published at the beginning of the V&V project, and the V&V work summary report should be summarized and published after the V&V work is completed.

Table 2. V&V tasks to be carried out in each stage of V&V activities

Phases and Activities and Tasks	Concept V&V	Requirements V&V	Design V&V	Implementation V&V	Test V&V
Risk analysis	✓	✓	✓	✓	✓
Standard performance analysis	✓	✓	✓	✓	✓
Traceability analysis	✓	✓	✓	✓	✓
Hazard analysis	✓	✓	✓	✓	✓
Security analysis	✓	✓	✓	✓	✓
Concept documentation evaluation	✓	NA	NA	NA	NA
Software requirements evaluation	NA	✓	NA	NA	NA
Software design evaluation	NA	NA	✓	NA	NA
Interface analysis	NA	✓	✓	✓	NA
Source Code Document Evaluation	NA	NA	NA	✓	NA
Unit Test Execution	NA	NA	NA	✓	NA
Test documentation evaluation	NA	NA	NA	NA	✓
System testing	NA	NA	NA	NA	✓

6 V&V Technology and Method

The V&V technology and method includes the integrated application of dynamic/static test methods and review/analysis/test technology of embedded V&V method in nuclear power plant, including: Document Review, Code Review, Traceability Analysis, FMEA, Code Static Analysis,, Black box testing, White box testing, etc.

The comprehensive application of dynamic/static testing methods combined with review/analysis/testing technologies, better meets the requirements of depth and breadth of activities and tasks of embedded V&V of security important system in nuclear power plant [4]. At the same time, it meets the principle requirements of diversified technical means in important fields of nuclear power safety [5].

Design check and traceability analysis realize 100% quality measurement of positive and negative traceability of embedded technology V&V requirements. An important task in the process of software testing is defect analysis, which can obtain the function module of defect aggregation, the distribution of defects with higher serious grades, the discovery trend and phase distribution of defects. Through defect analysis, the relationship between bug discovery trend and test cost could be clearly observed, as shown in Fig. 4. There are 4 commonly used defect parameters:

1) Status: the current status of the defect.
2) Priority: the relative importance of defects that must be addressed and resolved.
3) Severity: the degree to which the defect affects the end user, organization or third party.
4) Origin: the original fault and its location that caused the defect, or the component that needs to be repaired to eliminate the defect.

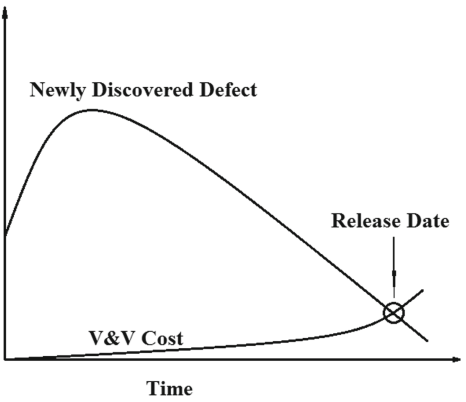

Fig. 4. Relationship between defect trend and cost

7 Application Effect

Software Contribution to Product Quality Improvement:

A total of 88 problems have been found in the cold water refrigeration unit software V&V project based on embedded technology. Typical problems include:

1) Software requirements would not reflect the requirements related to "parameter setting" user rights.
2) It fails to clearly reflect the interface relationship between function module.
3) The detailed implementation requirements for online upgrade are not reflected.
4) The response time exceeds the limit.

Recognition by Experts in Nuclear Power Field:

The cold water refrigeration unit software V&V project based on embedded technology is standardized, rigorous. It meets the requirements of independence, and conforms to the provisions of relevant laws and standards. Software V&V work effectively ensures the software quality of embedded technology products in the end, it meets the requirements of national regulatory authorities, and has good application and promotion value.

8 Conclusion

Through engineering practice, a new V&V method based on embedded technology is proposed in five dimensions: standard research, V&V scheme, V&V strategy, V&V activities and tasks, and V&V technologies and methods. Based on software abstract test, the relationship between defect trend and cost is analyzed. Specification-based tests and code-based unit-level tests are organically combined. Finally, it meets the requirements of national regulatory authorities, and has good application and promotion value.

References

1. IEC 61508-3: Functional safety of electronic/electronic/programmable electronic safety-related systems-Part 3: Software requirements (2010)
2. IEC 62138: Nuclear power plants-Instrumentation and control systems important to safety-Software aspects for computer-based systems performing category B or C functions (2004)
3. IEEE 1012: IEEE Standard for Software Verification and Validation (2004)
4. HAD 102/16: Systems Important to Safety Based on Computer of Nuclear Power Plants (2004)
5. HAF102: Regulation for Nuclear Power Plant Design Safety (2004)
6. Zhao, J., He, Y.-N., Gu, P.-F., Chen, W.-H., Gao, F.: Reliability of digital reactor protection system based on extenics. Springerplus **5**(1), 1–9 (2016). https://doi.org/10.1186/s40064-016-3618-y
7. 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: Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems (2017)
8. Gu, P.F., Liu, Z.M., Liang, H.H., et al.: Evaluation measures about software V&V of the safety digital I&C system in nuclear power plant. In: Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems (2018)