Proceedings of the Korean Nuclear Society Spring Meeting

Kori, Korea, May, 2000

Methodological Approach to Software V&V for the Reactor Protection System

Na Young Lee[1], Il Soon Hwang[1], Seung Rok Oh[2], Joong In Choi[3]

1)Seoul National University
Department of Nuclear Engineering
56-1, Shinlim-dong, Kwanak-Gu,
Seoul, Korea 151-742

2)Dankook University
Department of electronic engineering

3)Kyungwon university
Department of electrical, electronic engineering

Abstract

In the nuclear power industry, digital technology has been introduced only recently for the Instrumentation and Control(I&C) of reactor systems. Although the digital I&C system has many advantages over its analog counterpart, its application has drawn some safety issues such as software reliability, especially when applying it to nuclear power plant(NPP) safety systems. For this reason, the concept of verification & validation(V&V) was introduced. Among the V&V techniques, formal method is believed to be as advantageous for its strength in safety-critical characteristics. In this paper, we analyzed the available V&V techniques based on the formal method and discussed the possible options to compensate the shortcomings of the current formal method.

1. Introduction

During the 1960's and 1970's, digital technology began to assume an increasingly important role in large systems such as aerospace, national security, telecommunications, and energy applications. For the nuclear power industry, however, the conversion from analog technology to digital instrumentation and control systems started in the late 1980's and early 1990's[1]. This represents highly conservative attitude toward new technology among nuclear electric utilities.

Although a digital system possesses advantages over its analog counterpart, software reliability is the key issue especially when applying it to NPP safety systems. Therefore the concept of software verification and validation(V&V) was introduced to assure the reliability of safety critical systems.

At present, there is no proven, objective method to measure the reliability of a software-based product to the level of confidence required for safety-critical nuclear applications. In order to add further confidence, software V&V should promote a thorough and disciplined development process and thereby encourage thoughtful design and systematic cross-checks throughout the development cycle.

We reviewed and analyzed available V&V techniques and proposed a new approach to RPS in this paper.

2. Categorization of V&V techniques

In V&V, of particular importance is the form of expression used for the software requirements because most of the methods and tools at later stages in the life cycle can only be used provided that the appropriate requirements tool is used from the early stages. Furthermore, the very act of expressing requirements in a rigorous structure and format is itself an important part of requirements analysis.

V&V analysis methods can be categorized as shown in Fig. 1[1].

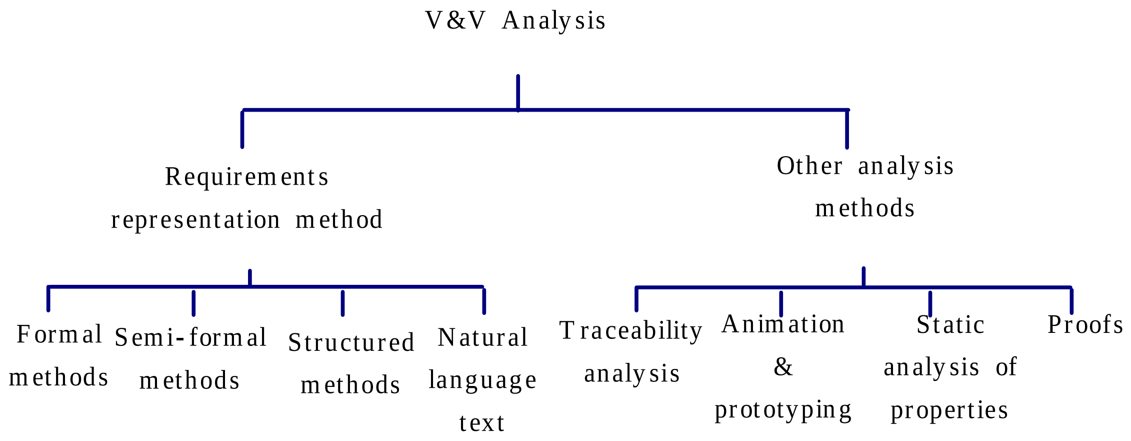

Fig. 1 V&V analysis techniques[1]

Among above methods, formal methods are mathematics-based techniques for describing system properties, and provide frameworks within which people can specify, develop and verify systems in a systematic, rather than ad hoc, manner. Semi-formal methods combine functional representation with graphical overview to show how the functions are tied together. They retain some of the mathematical rigor of the formal methods. However it require less mathematical competence to apply, and therefore, it is preferred choice for a variety of commercial software tools.

We reviewed literatures to identify the characteristics of some V&V analysis methods. This is summarized in Table 1[7]. In this table, V&V analysis methods are classified in three parts. In each classes, there are many available methods, we reported a few of them which are well known and applied satisfactorily to industry.

3. Choosing V&V method for the Application to RPS

The logic of RPS is based on the condition that defines whether or not a process parameter exceeds its predefined setpoint. If the logical combination of these conditions is satisfied, a scram action is initiated.

The Electric Power Research Institue(EPRI) classified nuclear I&C systems for digital I&C upgrades. The RPS is classified as the most safety-critical item because of the crucial role played by the RPS and short time response required of reactor trips. By classifying a system, the general requirements provided by standards can be transformed to

Table 1. Characteristics of V&V analysis methods

V&V classes	method	Description
1. Formal methods	Mathematical verification of requirements (Jones, 1986)	Translation of requirements into mathematical form for proving various properties
	Z(Chisholm, 1990)	A typed set-theoretic language employing mathematical expressions, schema, to describe aspects of a system; the schema consist of declarations grouped with property predicates about declarations
2. Semi-formal methods	Ward-Mellor Method (Ward, 1986)	An extension of structured analysis system specification techniques developed at Yourdan, Inc. for real-time systems, emphasizing data flow diagrams with control-flow annotations
	Petri-net Safety Analysis (Leveson&Stolzy, 1987)	Systems modeling with untimed(and timed) Petri nets to assure design adequacy for catastrophic-failure and other safety problems
3. Traceability assessments	Requirements tracing Analysis (NBS500-93, 1982)	Identification of individual requirement aspects and tracing of these to design aspects, and from the design to aspects of the implemented program

concrete recommendations for the appropriate approaches to design, verification and validation, and we can determine the level of activities needed to satisfy regulatory requirements.

For the RPS, some additional recommendations are made to add confidence from the point of view of both the utility and the NRC.[1]

1. Validation testing should include abnormal and faulted conditions. It should also include randomly generated test cases, to increase coverage and to avoid any manual bias in defining test cases.
2. Unambiguous formats, using tabular or mathematical representations, should be used to express required behavior in the requirements document. Reliance on natural language should be minimized.
3. More extensive structural testing should be performed to exercise each branch of each decision statement.
4. Reviewers should report to an organization separate from that of the developers.

Among V&V analysis methods, formal methods can best meet these requirements because the language is usually based on mathematical exactness and the ability for reasoning. In addition, if the problem can be specified mathematically, a program can be systematically generated so as to satisfy the specification. Nevertheless the application of formal methods to nuclear industry is shown to be difficult due to several shortcomings.

Based on EPRI-sponsored research project, experience with the formal languages, including Z specification are summarized as follows;[1]

-There is a scarcity of useful software tool to support for the formal languages

-Considerable high level training and experience are required to acquire adequate writing skill of Z language.

-Past industrial experiences have been largely confined to small problems or to highly specialized problems relating to definitions of protocols.

From the literature review, it becomes apparent that the development of more understandable and systematic V&V method is needed. We consider a combination of formal tabular methods and semi-formal graphical methods may have potential to meet the goal.

4. V&V procedure

Verification and validation activity should be performed at each steps of the development of the systems in their life cycle. Generally development procedure can be described as shown in Fig. 2.

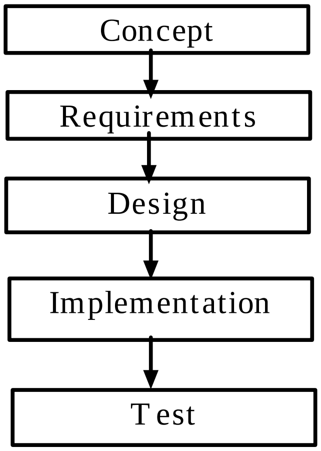

Fig. 2 General V&V procedure

Formal verification is the process showing, by means of formal deduction, that a formal design specification satisfies its formal requirements specification. The formal description of a design and its assumptions are used to define the premises, and the requirements are translated into the theorem that are to be proven. In hierarchical developments, assumptions and designs at one level become requirements at another, so the formal verification process can be repeated through many levels of design and abstraction. At the utmost level, validation must be carried out[3].

Detailed procedure using formal method can be summarized as following[4];

- Most of the system concept would be described as informal natural language requirements
- We should translate the informal requirements into formal requirements specification. At this stage we should choose a formal method that can satisfy the system classification level. As for RPS, it should satisfy Class 1 level of safety. From this process, we can identify and correct some of the deficiencies and ambiguities in the requirements written in natural language.
- Next step is the analysis of the requirements with pencil and paper, or using automatic theorem-prover by "If the specification is correct, the following property should be true." That is, when we put input into the formal specification, then output should provide an expected result. By using various input, we can find out some other errors which need some more detailed requirements. From this result, we can upgrade our informal natural requirements.
- Design should be verified. At this stage, the designer constructs a

high-level design specification and mapping function that relates the objects of the high-level design specification to the objects of the requirements-level specification which can be set from the high-level design data structure.

To show that the high-level design satisfies the requirements, we can use homomorphism as a proof method.

-From the well defined formal specification, we can generate the verification condition, and verify it. Code-level verification is usually the most time-consuming of all of the formal methods.

Upon completing all these verification procedure, the validation test is finally carried out for the developed software being embedded in the relevant hardwares. The validation process can be designed to cover a prescribed set of test conditions or a campaign of random test runs are made with a statistically defined performance goals.

5. Discussion

We reviewed some V&V analysis methods and their characteristics. Formal methods and semi formal methods have their own merits. They may not be sufficient when applied alnoe to RPS. Formal methods lacks automated tools, understandability, and easiness. Semi-formal methods do possess these qualities, however, the level of confidence and rigor needed in RPS is compromised.

A new approach that combines advantages of formal and semi formal method rapidly gains popularity in other industry.[5,6] One suggested hybrid languages which support an integrated specification of data structuring aspects, as well as functional and dynamic behavior. By combining sequential-oriented and process-oriented specification, mutual disadvantages can be compensated.[6] Another method is proposed to give a graphical appearance to formal methods, or alternatively, to add formal semantics to semi-formal graphical notations. In these approaches, specifications represented in semi-formal method partially translated into Z and enriched by formal annotations.

By using this approach, graphical overviews in semi-formal methods make the system more understandable, while mathematical expressions and scheme in formal methods make the system more reliable and rigorous in the verification. To use this approach, methodology should be studied including how to combine formal and semi formal method well and how to check the consistency between them to compensate their weakness.

6. Conclusion

In this paper, we examined the available concepts of V&V being introduced in nuclear industry with emphasis on its procedure using formal method. As RPS is a safety critical system its digital implementation needs the most rigorous verification method. Because the use of formal method or semi formal method alone may not fulfill all the requirement for RPS. For this reason, a new approach is suggested to combine formal and semi formal method such that all the required reliability can be satisfied. To explore this approach, thorough understanding of RPS characteristics and judicious choice of formal and semi-formal method is indispensable.

References

[1] EPRI, Handbook for verification and validation of digital systems Vol. 1 : Summary, 1994

[2] Akira Fukumoto et al. Application of algebraic specification to verify the design of safety logic in nuclear power plants, Nuclear technology, V. 124 N.3, pp 255-264, 1998

[3] John Rushby, Formal methods and their role in the certification of critical systems, Technical Report CSL-95-1, 1995

[4] Ricky W. Butler, Formal methods for life-critical software, AIAA computing in aerospace 9 conference, San Diego, Ca., Oct. 19-21, 1993, pp 319-329

[5] Yves Ledru, Complementing semi-formal specifications with Z, IEEE proceedings of KBSE, 1996, pp. 52-61

[6] Daniel Cooke, Languages for the specification of software, J. systems software, 1996, pp. 269-308

[7] Science applications international corporation, Guidelines for the verification and validation of expert system software and conventional software, Vol. 1, 1995