

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

Peng-Fei Gu^{1(✉)}, Zhe-Ming Liu², Hui-Hui Liang¹, Wei-Hua Chen¹, and Feng Gao¹

¹ 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
gupengfei@cgnpc.com.cn

² Product Information Committee of China Instrument and Control Society, Beijing, China
sss1116688@163.com

Abstract. Since the digital technology is used in the safety system of nuclear power plant (NPP), its safety and reliability are the most important factors to the safety operation of NPP. Software V&V (verification and validation) is a significant method to ensure the safety and reliability of the nuclear power safety I&C (instruments and control) system software, the system to evaluate the efficient of V&V activities needs to further research. An evaluation model of V&V activities has been described in the paper. The anomaly density, V&V effectiveness and V&V efficiency which are to measure the V&V effort, have been included in the model. In the article, the critical point of the anomaly density, V&V effectiveness, and V&V efficiency have been analyzed. Based on the V&V results of nuclear power safety I&C system software, a practice case has been performed to evaluate the V&V activities.

Keywords: NPP · Software V&V · Evaluation measures · I&C

1 Introduction

Computer technology has been quickly taken up in the process to improve and ensure the safety and reliability levels of nuclear power plants. The safety software of nuclear power plant has been divided into categories A, B and C [1]. The IEC 60880 [2] and IEC 62138 [3] together cover the domain of the software aspects of computer based systems used in nuclear power plants to perform functions important to safety. Software verification and validation (V&V) is the key element of evaluating the quality for the software. The verification and validation processes that are applied to the software life-cycle, including software concept V&V, requirements V&V, design V&V, construction V&V, and integration test V&V and so on [4]. TRS 384 [5] is the verification and validation technical report of software related to nuclear power plant instrument. IEEE 1012 [6] is the IEEE standard for system and software verification and Validation. The verification and validation activities are the most efficient method for evaluating the

software quality. They can help the users to evaluate the completeness, correctness, consistency and accuracy for safety software in nuclear power plant.

The standards and regulations are mature for the software verification and validation in nuclear power plant. The effective and sufficient of verification and validation activities also should be evaluated. The evaluation of verification and validation activities is benefit to improve the V&V processes and to appraise the software development processes and products. Some papers [7] have make the qualitative discussion. The related standards and regulations are less. IEEE 1012 [6] Annex E proposes three categories of measures associated with the V&V effort in brief. The measures are anomaly density, V&V effectiveness, and V&V efficiency. Trends can be identified and addressed by the feedback of V&V activities. But what the insightful information can be provided by the three categories of measures in the project. And how to use the three categories of measures in the practice needs to be considered.

An evaluate model of V&V activities has been described in the paper. The anomaly density, V&V effectiveness and V&V efficiency which are to measure the V&V effort, have been included in the model. This paper executes the quantitative research for evaluating the V&V activities. In the article, the focus opinions for the anomaly density, V&V effectiveness, and V&V efficiency have been analyzed. Based on the V&V results of nuclear power safety I&C system software, an calculate process has been performed for evaluating V&V activities, including the description for evaluating anomaly density, V&V effectiveness and V&V efficiency.

2 V&V Evaluation Model

Software V&V evaluation measures are based on the software V&V processes. Software V&V evaluation includes activities purpose building, data collection, data analysis and trend prediction. So an evaluation model of software V&V has been established in the paper as Fig. 1.

The model has been divided into six levels. The first level is the V&V object. The testers can make the V&V plan based on the object characteristics. The V&V processes, activities, and tasks have been included in the plan. The second level is V&V activities. It may need to execute multiple rounds. But the review items should be divided as the same principle during each round. The reviewed items are the third level. The reviewed items are difference in concept V&V, requirement V&V, design V&V, construction V&V and integration test V&V. The reviewed items are system requirements in the concept V&V for nuclear power plants. The items of other V&V processes are software requirements, design statements, implementation volume and test items. The quantitative information has been collected in the third and fourth levels. The forth level is anomalies. As Fig. 1, the concept anomalies may be found from the review of requirement, design, construction and integration test V&V. The requirements anomalies may be found from the review of design V&V, construction V&V and integration test V&V. It is the key point for calculating the V&V efficiency in the fifth level. The fifth level analyses the information based on the upper information. The anomaly density, V&V

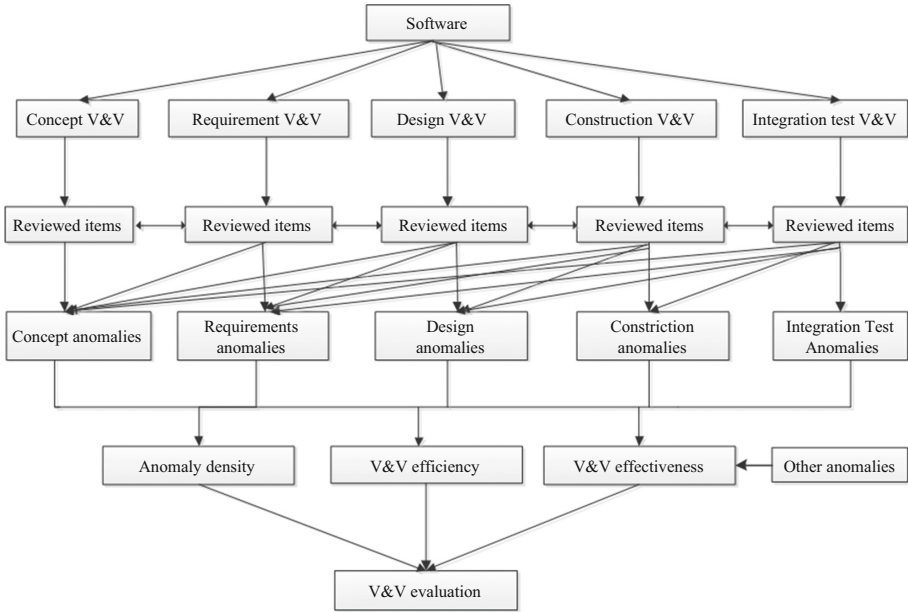


Fig. 1. Evaluation model of software V&V

efficiency and V&V effectiveness are the evaluation measures. The last level is V&V trend prediction.

3 V&V Evaluation Measures

3.1 Anomaly Density

Measures for evaluating anomaly density are used to evaluate the quality of the V&V effort. From IEEE 1012, the anomaly density is equal to anomalies found by V&V effort divide the reviewed items as Eq. (1). The anomalies include the concept anomalies, requirements anomalies, design statement anomalies, implementation anomalies and test anomalies found by V&V effort. So the concept anomaly density, requirements anomaly density, design anomaly density, implementation anomaly density and test anomaly density can be obtained.

$$\text{Anomaly density} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} \tag{1}$$

Anomaly density is influenced by anomalies found by V&V effort and reviewed items for every V&V phase. So if the baseline is changed, the density will be different in the same V&V phase. The principles of reviewed items should be kept uniformity in the same V&V phase.

Anomaly density trends of the same V&V phase can be used to judge the quality of the V&V activities. They also can provide the reference for the similar characteristics. The changing trend of the anomaly density may be caused by the new requirements and the unfound anomalies by V&V in the previous round. If the product increases the new requirements, the program development quality needs to be improved. If the new anomalies have been found in the behind round, the V&V processes should be evaluated.

3.2 V&V Effectiveness

The other category of measures associated with the V&V effort is the measure for assessing V&V effectiveness. From IEEE 1012, the V&V effectiveness is equal to anomalies found by V&V effort divide anomalies found by all sources. The all sources anomalies may come from V&V activities and the development effort. V&V effectiveness is a quantitative indication. The anomaly can be used to evaluate V&V activities separately. So the measure defined by Eq. (2) include the concept V&V effectiveness, requirements V&V effectiveness, design V&V effectiveness, implementation V&V effectiveness and test execution V&V effectiveness.

$$\text{V\&V effectiveness} = \frac{\text{Anomalies found by V\&V effort}}{\text{Anomalies found by all sources}} \quad (2)$$

Anomalies need to be measure in the same baseline between V&V activities and development effort. It's better to execute the V&V activities and development effort in parallelism. The anomalies found by all sources should be in the same reviewed items. So the anomalies found by the development effort need to be mapped in the V&V reviewed items. Then the V&V effectiveness is reasonable and believable.

If the V&V effectiveness is limit to one, then V&V activities is effective. If the V&V effectiveness is limit to zero, then the quality of the development is high. So the V&V effective can also provide the reference for V&V team to elevate the developer. It's benefit to predict the V&V schemes and cost.

3.3 V&V Efficiency

V&V efficiency is an important indication for evaluating the capability of the V&V effort. The requirement V&V efficiency is equal to requirements anomalies found by V&V in requirement activity divide requirements anomalies found by V&V in all activities as Eq. (3). Then the concept V&V efficiency, design V&V efficiency, implementation V&V efficiency and test execution V&V efficiency can be obtained in the same way.

$$\begin{aligned} &\text{Requirement V\&V efficiency} \\ &= \frac{\text{requirement anomalies found by V\&V in requirement activity}}{\text{requirement anomalies found by V\&V in all activities}} \end{aligned} \quad (3)$$

As Fig. 1, the requirements anomalies may be found from requirements V&V, design V&V, implementation V&V and test execution V&V activities. The V&V anomalies

need to be traced back to the primary causes. So the V&V anomalies should be discovered as early as possible to enhance the V&V efficiency. The quota means that the V&V activities are not separate. The V&V efficiency is related with the software life cycle.

Based on the V&V efficiency, the tester needs to find the factors which prevent the anomalies to be found. Then the V&V plan should be improved. The V&V activities need to be executed repeatedly to find the hidden anomalies and verify the new plan. V&V efficiency can also measure the development product. If the value is high, the factors may be that the development product and processes are immature.

4 V&V Evaluation Case

In order to verify the evaluation methods about software, a case has been exhibited. The evaluation measures of concept V&V activities have been performed of the safety digital I&C system in nuclear power plant. In the project, the concept V&V activity has been executed three rounds. The results show as Table 1. The change of reviewed items causes by the change of system requirements in the last round. Four system requirement documents has been became to one.

Table 1. The results of concept V&V activity

	Round I	Round II	Round III
Reviewed items	105	105	54
Anomalies	61	35	0

The baseline is as same as the round I of concept V&V. The anomalies obtained from the other V&V activities are shown as the Table 2.

Table 2. The anomalies of other V&V activities

V&V activities	Requirement V&V	Design V&V	Implementation V&V	Integration test V&V
Anomalies	6	0	0	3

4.1 Anomaly Density

The anomalies found by V&V activities decrease from the round I to round III. The concept anomalies found by V&V effort is seventy in the round I. They include the concept V&V anomalies of requirement V&V and test execution V&V. The round II anomalies are only come from the concept V&V. The anomaly density of the concept V&V activity is higher. The anomaly density has decreased along with the improvement of development process. So quality of the product and development process should be improved. The V&V activity facilitates correction of the anomalies. The quality of the V&V effort to discover anomalies is effective in the concept.

$$\text{Anomaly density I} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} = \frac{70}{105} = 0.67 \tag{4}$$

$$\text{Anomaly density II} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} = \frac{35}{105} = 0.33 \quad (5)$$

$$\text{Anomaly density III} = \frac{\text{Anomalies found by V\&V effort}}{\text{Reviewed items}} = \frac{0}{54} = 0 \quad (6)$$

4.2 V&V Effectiveness

The anomalies which come from the other source is less than V&V activities. The anomalies that have been found by development are included by the V&V activities. So the concept anomalies found by V&V effort is equal to the concept anomalies found by all sources. So the V&V effort is effective. The testers need to consider to incremental changes to the V&V process. The developers should concern to improvement the development process.

$$\text{V\&V effectiveness} = \frac{\text{Anomalies found by V\&V effort}}{\text{Anomalies found by all sources}} = \frac{70}{70} = 1 \quad (7)$$

4.3 V&V Efficiency

The V&V efficiency measure value is high that the V&V effort has discovered anomalies in the earliest concept V&V activities. The concept V&V process can decrease the rework and development costs. Combining the anomaly density with the efficiency, the development products need to further improve, the V&V effort is effective in concept V&V activities.

$$\begin{aligned} &\text{Concept V\&V efficiency} \\ &= \frac{\text{Concept anomalies found by V\&V in concept activity}}{\text{Concept anomalies found by V\&V in all activities}} \\ &= \frac{61}{70} = 0.87 \end{aligned} \quad (8)$$

The concept anomalies found by V&V in requirement V&V activity are caused by the concept documents are not detail. The requirements cannot trace to the concept document. The concept anomalies found by V&V in test V&V activity is that part of the parameter range is not explicit.

5 Conclusions

The evaluation model has been built in the article. The evaluation methods about software V&V of the safety digital system have been discussed in nuclear power plant. The paper has given the critical point of V&V anomaly density, V&V effectiveness and the V&V efficiency. The mapping between the reviewed items of the V&V activities and the anomalies found by all source or all V&V activities is the key point to obtain the exactly

evaluation value of V&V activities. The practice case is performed in the last. By the practical case analysis, the evaluation methods are effective to elevate the V&V effort.

References

1. IEC 61226: Nuclear power plants-Instrumentation and control systems important to safety – classification of instrumentation and control functions. International Electrotechnical Commission (2005)
2. IEC 60880: Nuclear power plants - Instrumentation and control systems important to safety – software aspects for computer – based systems performing category a functions. International Electrotechnical Commission (2006)
3. IEC 61138: Nuclear power plants - instrumentation and control important for safety – software aspects for computer – based systems performing category B or C functions. International Electrotechnical Commission (2004)
4. Gu, P., Wang, S.C., Chen, W.H., et al.: A study about safety I&C system software V&V in nuclear power plant. In: Proceedings of the 24th International Conference on Nuclear Engineering (2016)
5. TRS 384: Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control. International Atomic Energy Agency, Vienna (1999)
6. IEEE 1012: IEEE Standard for System and Software Verification and validation. The Institute of Electrical and Electronics Engineers (2012)
7. 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. Lecture Notes in Electrical Engineering (2016)