Discussion on the Software V&V Technology in Nuclear Power Plants

Hui-Hui Liang(✉), Wang-Ping Ye, Wei Liu, and Jian-Zhong Tang

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment,
I&C Equipemnt Qualification and Software V&V Laboratory,
China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
lianghuihuijilin@yeah.net

Abstract. Software V&V technology provides reliability and safety guarantee for digital system and intelligent equipment which used in nuclear power plant. Although a systematic scheme of software V&V technologies has been formed for nuclear power plant, there are some technical nodes need to be discussed and considered. The software V&V standard has been updated. The higher requirements are put forward for the depth, scope, the appropriate techniques and methods of the software V&V. This paper will discuss the upgraded version of software V&V related standards, and give the key points that software V&V technology needs to pay attention. Then the pre-development software identification, new software V&V technical of the special instrument and control system, and the applicability assessment of the safety analysis software are also been discussed. The technical difficulties faced by software V&V in the above aspects will be put forward. At last the future development direction of software V&V technology is proposed.

Keywords: Software V&V · PDS · Software assessment · NPPs

1 Introduction

The digital technology has been used in the Nuclear Power Plants (NPPs). To ensure the reliability and safety of digital technology used in the Nuclear Power Plants, the software development shall meet the requirements of rigorous standards and regulations. Such as the software for performing category A functions should comply with the IEC 60880 or IEC 62566 [1, 2], the category B and C need to follow the IEC 62138 in the nuclear power plants [3]. The software can also be divided into pre-developed and new developed software. And the nuclear power plant safety analysis and calculation software and the software for special instrument control system belong to another classification. So the software quality assessment is difficult and complex. The software verification and validation (V&V) technology is widely accepted and effective method to ensure the software quality in the nuclear power plants [3]. In recent years, the regulations and standard s related to the nuclear power plants software safety has been updated and released. The IEEE 1012-2014 is the core criteria which the software V&V activities is based on, has been update to IEEE 2017. IAEA has adjusted the regulation and standards.

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 380–385, 2021.
https://doi.org/10.1007/978-981-16-3456-7_36

SSG - 39 of the safety standards related to instrument control system and software design entered into force in 2016. RCC-E has been upgraded to 2106. Furthermore, higher requirements are put forward for the depth, scope, the appropriate techniques and methods of the software V&V.

Although the software V&V technology has been used in power plants construction objects, there are some technical nodes need to be discussed and considered. The pre-developed software (PDS) and new software identification, and calculation software assessment used for safety analysis in nuclear power plants will be discussed in the paper. Then the development trend of the software V&V technology will be proposed.

2 Standard Requirements

In recent years, the relevant standards for software V&V have been upgraded, which put forward new requirements for software V&V activities in nuclear power plant. NRC puts forward an endorsement through R.G. 1.168-2013 that software V&V requirements for nuclear safety class shall be subject to IEEE 1012-2004 Integrity Class 4 [1, 2]. The standard scope of IEEE 1012-2004 is limited to software V&V, while IEEE 1012-2012 and IEEE 1012-2017 extend the scope of V&V to systems and hardware [3, 4]. In IEEE 1012-2017, new requirements have been added for V&V tasks related to hazard analysis, security analysis, and evaluation of source code and source code documentation during the design, implementation, testing, installation, operation and maintenance phases.

The main changes of newly published security standard SSG 39-2016 in IAEA involve the continuous development of computer applications and the evolution of methods required for safety [5], security and actual use. In addition, the development of the Human Factors Engineering and the needs of computer information security are also considered. The requirements for software V&V of RCC-E 2016 are mainly based on IEC standard series (IEC 60880, IEC 62138, IEC 62566) [6]. RCC-E 2016 supplies some requirements which have not listed in the IEC standard.

RCC-E-2016 Volume III Part E has supplied or modified the software V&V requirements of software aspects for computer-based systems performing category a functions. The requirements include verification plan, software aspects confirmed by the system, software modification, defense against common cause failure in software, and identification requirements for limited function digital equipment (DDLF). The changes of NS-TAST-GD-046 (rev4, 2017) and NS-TAST-GD-046 (rev5, DRAFT) versions mainly include the scope of application [7], multi-legged demonstration, and the addition of pre-development items, such as the identification requirements for commercial-grade intelligent equipment and platforms.

Compared with the existing software V&V technical scheme, it can be seen that the existing software V&V scheme basically covers and meets the new requirements of relevant laws and standards, but the following contents need to be paid attention to in terms of specific implementation details and depth,

- Strengthen the V&V work of project planning and Configuration Management, and refine its implementation strategy
- Strengthen tool appraisal requirements and related tasks, and refine their implementation strategies;

- Refine the implementation strategy of hazard analysis and security precaution analysis tasks;
- Analyze the application scope of statistical tests, formalize methods, and propose determine specific implementation plans when conditions permit.

3 Technical Discussions

Based on Sect. 2, although the software V&V technology has been used in power plants construction objects, there are some technical nodes need to be discussed and considered. The pre-developed software identification, statistical tests and formalizes methods which used to the new software V&V, and calculation software assessment which used for safety analysis are the difficult points in software V&V activities is in nuclear power plants.

3.1 Pre-developed Software Identification

More and more equipment in nuclear power plants includes digital software. These intelligent devices have the advantages of high control precision, strong calculation capability, high data transmission reliability, easy expansion and configuration, easy maintenance and management, high integration, etc., which greatly improve the economic benefits of Nuclear Power Plant when digital devices are used to perform Safety Function. Due to the high safety and reliability requirements of nuclear power plant, the newly developed software has high cost and long cycle, which cannot meet the application requirements of nuclear power projects in time.

Pre-developed software is that software is already exists and available as a commercial or proprietary product, and being considered for use [8]. Comparing with conventional industries, the nuclear power application market is smaller. At present, most of the pre-developed software rights are universal mature products and non-nuclear power customized products. The quality and technical standards which adopted by software supply contractor and development company are usually industrial standards. And whether the software functions are suitable for the expected application of nuclear power needs to be evaluated. So, how to prove that the pre-development software meets the software quality assurance and technical requirements is a key problem when using the existing mature pre-developed software to implement nuclear power plant safety-class functions.

According to the standard requirements, the applicability of the pre-developed software can be proved through standard conformity analysis, suitability evaluation, quality evaluation, operation experience feedback and supplementary testing activities. The difficulty is that the quality assurance records of pre-developed software are commonly incomplete. When the activities of quality assurance and configuration management cannot fully proof the pre- developed software satisfied the requirements of the nuclear power plants. Therefore, comprehensive suitability assessment is needed in combination with sufficient supplementary tests and good operating experience data.

3.2 New Software V&V

Under the new situation of nuclear power development, China needs to gradually have the ability to independently design and manufacture key equipment, only in this way the nuclear power "going global" can be realized. Nuclear Safety-class special system with independent intellectual property rights is an important technology to be conquered in the research and development of nuclear power equipment. According to the requirements of laws and regulations, software V&V is an essential and important step to form nuclear safety-class special instrumentation and control system products. Software V&V technology mainly includes review technology, analysis technology and testing technology. But the traditional testing technology is difficult to achieve 100% full path coverage test and cannot identify all potential errors.

The formal verification technology is based on mathematical logic reasoning and has rigor mathematical and completeness logical in system modeling and testing. Formal verification can realize 100% full path coverage testing, thus making up for the deficiency that traditional testing technology is difficult to find all software defects. This verification technology is beneficial to improve the depth of software V&V and the quality of software.

Another difficulty with software V&V is statistical testing. Statistical testing is a key technology to quantitatively evaluate the reliability of nuclear power plants software. Statistical testing can test and evaluate the reliability and safety of safety-important instrumentation and control system design in the early stage of project construction by simulating actual operating conditions so as to find defects and problems as early as possible and avoid the risks of project delay and high repair costs caused by finding problems only during the on-site commissioning phase.

Standards such as IEC 60880, IEC 61508 and IEEE 1012 and reports of international authoritative organizations highly recommend formal methods and statistical tests for design verification of nuclear safety-class instrumentation and Control systems [8, 9]. In order to ensure the security and reliability of the special instrumentation and control system designed by nuclear power plant self-reliance and to meet the requirements of the project going global, it is necessary to start the relevant work of formal verification and statistical testing as soon as possible. At present, it has not form a good formal verification and statistical testing scheme in nuclear power plant.

3.3 Calculation Software Used for Safety Analysis

The computer software used in the safety analysis of nuclear power plants usually includes 9 categories, such as radiological analysis program, neutron physics program, fuel behavior program, thermal hydraulic program and probabilistic safety analysis program. According to the requirements of HAF 102-2004 and HAD 102/17-2006, the computer program, analysis method and nuclear power plant model applied in Safety Analysis must be verified and validated, and the uncertainty must be fully considered. The software verification and validation of nuclear power plant safety analysis evaluation procedure requires not only requirements verification, design verification, implementation verification, and test verification, the most important thing is carrying out the verification and validation of model evaluation, which is also the difficulty and key work for calculation software used for safety analysis nuclear in power plant.

The evaluation model for safety analysis needs model assessment, and appropriate data (experimental data, international standard questions, nuclear power plant operation data, etc.) also need to be used to prove the suitability of the evaluation model to simulate the behavior of nuclear power plant during assumed transients and accidents.

Software finally confirmed that it must be compared with experimental and power plant data. If the calculation method in Safety Analysis contains a large number of simplifications, if possible, more advanced calculation methods should be adopted to prove that the main physical phenomena have been fully considered in the simplified method. Software finally validation testing data must be compared with experimental and power plant data. If the calculation method in Safety Analysis contains a large number of simplifications, if possible, more advanced calculation methods should be adopted to prove that the main physical phenomena have been fully considered in the simplified method.

4 Development Trend of Software V&V

With the development of various emerging technologies, the software V&V development of nuclear power plants will focus on following aspects in the future. Agile testing is a series of testing practices that conform to agile development methods and strive to achieve quality and efficiency. Automation focuses on the automation of testing, including the development of testing tools and the optimization of testing activities, transforming human-driven testing behavior into a behavior executed by machines. Testers can log in to the testing environment to carry out testing services. Servicing is to make software a service and build a test platform so that software developers can automatically acquire the ability to test on demand. Modeling is a model-based test, which is more effective and accurate, and the test can be completely automated. Intelligence is to use the Internet, storage capacity, technical capacity and big data computing to carry out automatic generation of test data, independently control software, intelligent analysis of defects and logs, and optimize testing and design. Cloud platform is a foundation facility for testing, which can better support automation, service and intelligence.

5 Summary

The software V&V technology in nuclear power plants need to strictly comply with the requirements of regulations and standards. Formal verification and statistical testing methods are the bottlenecks that restrict nuclear power to go global at present. It is also an important topic for the computational software used in Safety Analysis to formulate an effective model correctness and uncertainty evaluation scheme. Agility, automation, modeling and intelligence are the development trend for the software testing. The software V&V of nuclear power plants need to carry out the above-mentioned cutting-edge technology research to improve the software quality and testing efficiency.

References

1. R.G.1.168-2013. Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (2013)
2. IEEE 1012-2004. IEEE Standard for Software Verification and Validation (2004)
3. IEEE 1012-2012. IEEE Standard for System and Software Verification and Validation (2012)
4. IEEE 1012–2017. IEEE Standard for System, Software and Hardware Verification and Validation (2017)
5. SSG-39-2016. Design of Instrumentation and Control Systems for Nuclear Power Plants (2016)
6. RCC-E-2016. Design And Construction Rules for Electrical And I&C Systems And Equipment (2016)
7. NS-TAST-GD-046.R4-2017. Computer Based Safety Systems (2017)
8. IEC 60880-2006. Nuclear Power Plants-Instrumentation and Control Systems Important to Safety-Software Aspects for Computer-Based Systems Performing Category a Functions. Switzerland (2006)
9. IEC 61508-2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (2010)