Research on the Verification and Validation Method of Commercial Grade Software in Nuclear Power Plants

Wang-Ping Ye(✉), Ya-Nan He, Peng-Fei Gu, and Wei-Hua Chen

State Key Laboratory of Nuclear Power Safety Monitoring Technology and Equipment, I&C Equipment Qualification and Software V&V Laboratory, China Nuclear Power Engineering Co., Ltd., Shenzhen 518172, Guangdong, China
yewangping@126.com

Abstract. With the development of digital technology in nuclear power plants, more and more commercial grade software is being widely used in nuclear power plants. However, there has not been formed a unified dedication standards at domestic and overseas, which not only brings certain difficulties for dedication, but also has a certain impact on the safety of nuclear power plants. Based on the analysis of related standards at domestic and overseas, combined with the software V&V experience in practical work, this paper presents a set of practical Commercial grade software dedication methods. It can not only guide the dedication of Commercial grade software of China's nuclear power plants, but also can provide a reference for the dedication of commercial grade software of HPR1000.

Keywords: Nuclear power plant · Commercial grade software · Verification and validation · Dedication

1 Introduction

With the continuous development of China's nuclear power technology, more and more digital devices are being applied to nuclear power plants. Smaller devices such as smart devices that transmit pressure and level signals, and larger scaled safety digital instrumentation systems, are increasingly used in the design, construction, operation, and maintenance of nuclear power plants.

In the past, most of the software used in nuclear power plants was costly imported which mainly through commercial purchase, such as Mitsubishi's I&C system TXP, TXS, Siemens's industrial software SMATIC S7. However, in recent years, with the process of "going out" and autonomy of China's nuclear power technology, more and more independent research & development software has been used in nuclear power plants, such as the safety I&C system FirmSys which developed by the China Techenergy CO., LTD. Even some safety analysis software has also been gradually localized, such as the neutron transport calculation software SUPERMC which developed by the Chinese Academy of Sciences Security, also the development of non-safety-critical software. In addition, with the mass construction of nuclear power plants,

© Springer Nature Singapore Pte Ltd. 2019
Y. Xu et al. (Eds.): *Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems*, LNEE 507, pp. 139–148, 2019.
https://doi.org/10.1007/978-981-13-3113-8_16

digital equipment in the general industry is gradually applied to nuclear power plants, such as embedded devices PLC, FPGA etc.

Although a large amount of manpower and resources have been devoted to independent research and development, the gap between China's software industry and foreign software is unavoidable. At the same time, domestic software lacks long-running operating experience compared to foreign software, and the safety should be great concerned. At the same time, in order to save development costs or shorten progress, self-developed equipment often use some not fully verified commercial grade software in the R&D process, and also use components that are not available from the source code, such as operating systems in embedded devices, further increases the safety risk of the software. For safety-critical autonomous software used in nuclear power plants, such as DCS, with strict development process, perfect quality assurance and fully third-party verification and validation, such as white box testing with 100% coverage, the software quality is credible [5]. However, for commercial grade software, considering the development costs, it is generally not a perfect development process and quality assurance. If be applied directly in nuclear power plants, the consequences would be unimaginable.

How to dedicate these commercial grade software to meet the review requirements of domestic and foreign regulatory agencies has become a problem that needs to be solved urgently, also no engineering experience can be used for reference. Based on the analysis of commercial grade software dedication standards, this article proposes a set of concrete and feasible commercial grade software V&V solutions draw from the engineering experience of safety software identification of the nuclear power plants. It mainly includes the following parts: The first part briefly introduces the status of application and appraisal of commercial grade software in nuclear power plants; the second part mainly introduces the differences and connections between commercial grade software and safety software, and the focus and difficulty of commercial grade software dedication; the third part analyzes and combs domestic and foreign commercial grade software related standards, and gives a reference to the V&V method; the fourth part gives a feasible V&V plan, its advantages and disadvantages combining with the standards analysis results and engineering practice. The fifth part combed and summarized the content of the plan needs to be improved and the follow-up research. The sixth part lists the reference literature information referenced in the writing process.

2 Commercial Grade Software

2.1 Definition

Commercial grade software refers to the software used in commercial grade items, including system software and application software. Commercial grade items refer to structures, systems or components that do not design and manufacture under a nuclear quality assurance program but affect the safety functions of the plant. In general, it is not the items specifically designed for nuclear facilities but used in nuclear power plants. Such items are generally not subjected to the same stringent process control and verification as nuclear-level items during the design and development process [6].

2.2 Differences and Connections

The software used in nuclear power plants is divided into pre-developed software and newly developed software. Pre-developed software is Commercial Off-The-Shelf software that has been developed and is generally not specifically developed for nuclear power plants, and commercial grade software belongs to this category. New software refers to that software designed and developed specifically for nuclear power plants. There are two classification methods for the new software: IEC and IEEE. According to the importance of the functions performed by the software and the severity of its failure, the IEC classifies the software into categories A, B and C. For example, the failure of Class A software can cause catastrophic consequences such as radioactive leaks; the IEEE classifies software into integrity level 1, 2, 3, and 4 based on the risk of failure, with integrity level 4 being the highest and equivalent to IEC Class A.

2.3 Difficulty of V&V

The main difficulty in the dedication of commercial grade software is that there are no unified standards to guide the related work. On the other hand, there are often irregular documentation, lack of quality assurance, configuration management and software source code during the development and dedication of commercial grade software.

3 Analysis of V&V Standards

3.1 Standard Classification

For the application of commercial grade software in nuclear power plants, the main standards are the international standard IEC series and the United States standard. Among them, international standards IEC 60880 and IEC 62138 present the requirements for the dedication of Class A and B, C commercial grade software [3, 4]. The US standard also has a complete standard system and detailed requirements for the dedication of commercial grade software. Table 1 provides the details.

3.2 Interpretation of Standards

3.2.1 IEC Standards

IEC 60880 and IEC 62138 are consistent in the process of dedication of commercial grade software, but differ only in depth. See Table 2 for details. One or more of the dedication content may be used to prove the correctness of the software according to the assessment.

Table 1. Commercial grade software dedication standards

Level	Title	Document No.
Laws and Regulations	Reporting of Defects and Noncompliance	10CFR21,1995
	Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants	10CFR50, Appendix B
Nuclear Safety Guidelines, Requirements and Inspection Procedure	Standard Review Plan	USNRC NUREG 0800
	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	R.G.1.152-2011
	Inspection Commercial-Grade Dedication Programs	NRC Inspection Procedure 43004
	Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products	USNRC Generic Letter 89-02 1989
	Licensee Commercial-Grade Procurement and Dedication Programs	USNRC Generic Letter 91-05 1991
Industrial Standards and Technical Reports	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations	IEEE 7.4.3.2-2010
	IEEE Standard for Software Verification and Validation	IEEE 1012-2004
	Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications	EPRI NP-5652 1998
	Supplemental Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items	EPRI TR-102260 1994
	Guideline of Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications	EPRI TR-106439 1996
	A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications	NUREG/CR 6421 1996

Table 2. Commercial grade software dedication requirements

Dedication content	Class A software	Class B software	Class C software
Standard compliance analysis	√	√	√
Suitability evaluation	√	√	×
Quality assessment	√	×	×
Operational experience feedback	√	√	×
Supplementary test	√	√	×

3.2.2 IEEE 1012

IEEE-1012 Appendix D provides more detailed options and suggestions for the verification and validation of reuse software (software libraries, custom software developed for other applications, COTS software, and existing software), and is mainly divided into two areas [2].

First, the critical analysis method is used to assign the integrity level of the software, and then determine the minimum V&V tasks to be performed by the software identification according to the standard. For example, when the software integrity level is 3 and 4, it is necessary to carry out hazard analysis and risk analysis, but when the software integrity level is 1 and 2, there is no need.

Then, when the development documents and information of the software are complete and available, V&V tasks of each stage needs to be carried out according to the minimum task set, such as Concept V&V, Requirement V&V etc., the specific V&V process suggested in Fig. 1.

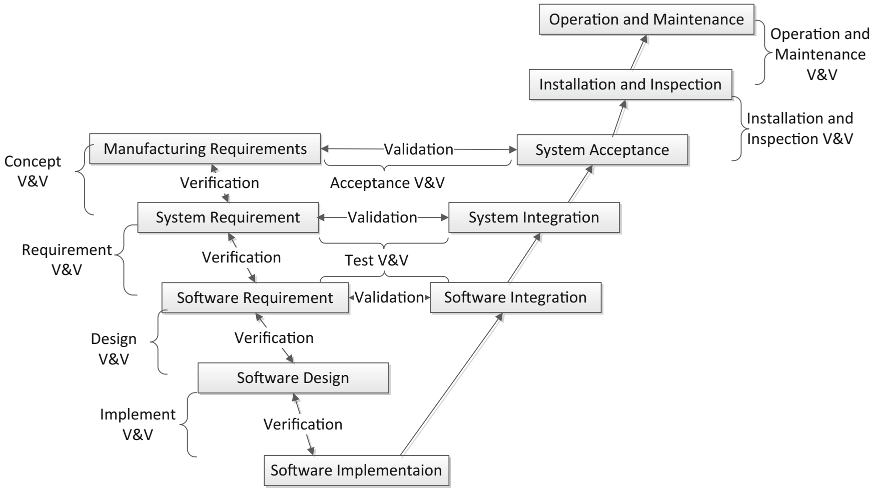

Fig. 1. Software V&V process

When the V&V inputs like documents and codes required for carrying out the minimum tasks in each stage are not available and the software requires high confidence, substitute analysis and test methods should be permitted instead of the IEEE 1012 requirement V&V tasks to generate objective conclusions about the correctness, completeness, accuracy and usability of the reused software. The following alternative methods should be considered (decreasing as desired):

a) Black box testing.
b) Review developer's quality assurance.
c) Operational history.
d) Audit results.
e) Artifacts.
f) Reverse compilation.
g) Prototyping.
h) Prior system results.

3.2.3 IEEE 7.4-3.2

IEEE Std. 7-4.3.2-2010 Section 5.17 provides guidance on how the commercial-off-the-shelf (COTS) digital equipment which not developed under a nuclear quality assurance program and performing the intended safety functions can meet the nuclear power plant's dedication process [1]. The terms and provisions for the commercial grade dedication of digital equipment are basically the same as those in the EPRI reports. According to the requirements of this standard, the dedication process for digital equipment consists of preparation phase, performing phase, and design review phase. The detailed requirements for each phase are shown in Table 3.

Table 3. Dedication process and requirements

Identification process	Identification requirements
Preparation phase	1. Use effects analysis (FMEA) and fault tree analysis (FTA) to identify the potential risks and hazards that may interfere with COTS item to achieve their safety functions; 2. Identify the safety functions performed by COTS item and conduct dedication, including performance requirements, accuracy, time response, system integrity, and configurability or programmability; 3. Evaluate the computer security risks and hazards associated with the system, including impact on hardware, software, interfaces to other systems, and life cycle documentation, as well as plant procedures for the COTS items to determine if the risk is acceptable.
Performing phase	1. Developing detailed acceptance criteria, including physical characteristics, performance characteristics, and development process characteristics such as software model and version numbers, response time, and traceability; 2. Determine the acceptance method, such as special test, commercial grade survey, source verification, evaluation, etc.
Design review phase	1. Evaluate the life cycle process, including design, development, quality assurance, review, testing, configuration management and change control; 2. Evaluate failure modes and effects analysis of vendor or dedicating entity; 3. Evaluate the operating history in similar safety critical applications.

3.2.4 EPEI NP-5652

EPRI NP-5652 is the main report of commercial grand dedication (CGD), in which EPRI describes the background, objectives, basic concepts, overall processes and basic methods of CGD, and proposes a dedication method consisting of technical assessment and acceptance. The main task of CGD is to verify and evaluate the critical characteristics of the project using appropriate acceptance methods. See Table 3 for details. Critical characteristics often include physical and performance characteristics, depending on safety features, environmental conditions, and item failure mechanisms (Table 4).

Table 4. CGD appraisal process and requirements

Dedication process	Dedication requirements
Technical assessment	Identify safety functions
	Failure modes and effects analysis (FMEA)
	Identify critical characteristics
Acceptance method	Special tests and inspections
	Commercial grand survey
	Source verification
	Item/supplier performance record

3.2.5 EPRI NP-106439

This report refers to the four methods of commercial grade item dedication proposed by EPRI NP-5652 to evaluate the critical characteristics of commercial digital equipment. This report classifies the critical characteristics of commercial digital devices into three major categories, physical characteristics, performance characteristics, and dependability characteristics, and provides examples of verification methods and acceptance criteria for various types of characteristics. Through the verification of these characteristics, it is possible to evaluate whether commercial digital equipment (including software) meets the needs of nuclear power plant related safety functions. Specific requirements are detailed in Table 5.

Table 5. Identification process and requirements

Critical Characteristics	Acceptance object	Acceptance method
Physical characteristics	Hardware	Verification through inspection and measurement
	Software	Identify requirements for expected and unexpected functions
Performance characteristics	Response time, progress and other performance indicators	Testing
		Design review
		Failure analysis
		Operating history review
Dependability characteristics	Hardware	Seismic test, EMC, aging and other hardware identification
	Software	Evaluation of software development and quality assurance processes, including evaluation of V&V processes, configuration management, and operational records

3.3 Summary and Analysis

Through the analysis of above-mentioned standard's requirements, commercial grade item dedication is basically the same in requirements and methods. Both require the completion of commercial grade dedication through evaluation of critical characteristics, development process quality records (including V&V, configuration management records), and operation records. Among them, software is the focus of quality control in digital commercial grade items [7, 9]. The most effective and direct method is to conduct software independent verification and validation (V&V).

Because the equipment suppliers in the design and development process of commercial grade software generally follow the industrial standards, the records, documents, reports, etc. of the development process are often incomplete or do not fully meet the requirements of the nuclear industry standards, and may not be able to carry out the software entire life cycle V&V. Therefore, an alternative analysis must be taken to comprehensively evaluate the QA operational status, performance, and operational feedback of commercial grade items, in order to make better judgments on software quality.

4 V&V Method

4.1 V&V Plan

Although the standards have made corresponding requirements for the evaluation of commercial grade software, but each standard has different emphasis. IEEE 1012 focuses on the verification and validation of the software entire lifecycle, and gives the minimum set of tasks and V&V requirements for each software V&V phase, which is suitable for the identification of software with complete development documents and data. EPRI NP-5652 provides an evaluation and acceptance method for commercial grade software and it is suitable for the dedication of incomplete or hard-to-get software. IEC 60880 and IEC 62138 require both.

Combined with engineering experience, the IEEE 1012 is more performable than other standards in the V&V of the software entire life cycle. IEC 60880 and IEC 62138 are superior to EPRI NP-5652 in terms of evaluation and acceptance.

4.2 Cases

The software of the non-safety control system used in nuclear power plants developed by a non-nuclear enterprise in China who carries out software development and quality assurance of the entire life cycle according to the waterfall model, and the relevant development documents and data are complete [8, 10]. For this software, the corresponding V&V work is carried out in accordance with the requirements of the IEEE 1012 integrity level 2, and the specific V&V flow and tasks are shown in Table 6.

The control software of a foreign smart device is intended to be applied to a domestic nuclear power plant. The software belongs to category A and needs to be identified accordingly. However, due to confidentiality and other requirements, it is impossible to provide complete software data for independent identification throughout

Table 6. V&V phases and tasks

V&V phase	V&V tasks	V&V method
Concept V&V	Concept document evaluation, traceability analysis, security analysis	Document review
Requirement V&V	Requirements document evaluation, traceability analysis, safety precaution analysis	Document review
Design V&V	Design document evaluation, traceability analysis, safety precaution analysis	Document review
Implement V&V	Source code and document evaluation, traceability Analysis, security analysis, unit testing	Document review, static analysis, White box testing
Test V&V	Integration test, system test	Black box testing

the entire life cycle [11]. Finally, according to the requirements of IEC 60880, the foreign software was subjected to the identification of standards compliance, operational experience evaluation, and supplementary testing to verify whether the software meets the requirements of Class A software [12].

5 Summary

Although IEC and United States have given corresponding requirements and methods for the dedication of commercial grade software and have certain enforceability. However, the supervision and dedication of commercial grade software in China is still insufficient at now, and more in-depth research is needed to carry out.

At the same time, with the departure of HPR1000, due to the lack of successful experience, there is still some uncertainty in how to prove the dedication of the software is sufficient to meet the GDA and EUR review requirements. More exchanges and discussions are needed.

References

1. Nuclear Power Engineering Committee of the IEEE Power Engineering Committee: IEEE 7-4.3.2. IEEE standard criteria for digital computers in safety systems of nuclear power generating stations. Institute of Electrical and Electronics Engineers, New York (2010)
2. Software Engineering Standards Committee of the IEEE Computer Society: IEEE 1012. IEEE standard for software verification and validation. Institute of Electrical and Electronics Engineer, New York (2004)
3. International Electrotechnical Commission: IEC 60880. Nuclear power plants instrumentation and control systems important to safety software aspects for computer based systems performing category A functions (2006)
4. International Electrotechnical Commission: IEC 62138, Nuclear power plants-instrumentation and control systems important for safety-software aspect for computer-based systems performing category B or C functions (2004)

5. Ye, W.P., Tang, J.Z., Chen, W.H.: Software V&V methods for safety digital I&C system of nuclear power plants. At. Energy Sci. Technol. **49**(zengkan1), 377–381 (2015)
6. Gu, P.F., Wang S, Chen, W.H.: A study about safety I&C system software V&V in nuclear power plant. In: International Conference on Nuclear Engineering (2016). V001T04A005
7. He, Y.N., Gu, P.F., Xi, W.: Research on status monitoring and reliability prediction method of digital control system for nuclear power plant. At. Energy Sci. Technol. **51**(12), 2338–2343 (2017)
8. Liang, H.H., Gu, P.F., Tang, J.Z.: The Software Security Analysis for Digital Instrumentation and Control Systems of NPPs. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems (2018)
9. Zhao, J., He, Y.N., Gu, P.F.: Reliability of digital reactor protection system based on extenics. SpringerPlus **5**(1), 1953 (2016)
10. Liang, H.H., Gu, P.F., Tang, J.Z.: A Study of Implementation V&V Activities for Safety Software in the Nuclear Power Plant. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems (2017)
11. Gu, P.F., Liu, Z.M., Liang, H.H.: Evaluation Measures about Software V&V of the Safety Digital I&C System in Nuclear Power Plant. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems (2018)
12. Xi, W., Gu, P.F., Liu, W.: A Study and Application about Software V&V Requirement Management Scheme in Digital RPS. Nuclear Power Plants: Innovative Technologies for Instrumentation and Control Systems (2018)