Research About Software Verification and Validation of Control and Protection System for Chinese Heavy-Duty Gas Turbine

Peng-Fei Gu[1], Zhe-Ming Liu[1,2], He-Ming Bao[1(✉)], Tao Bai[1], and Xue-Fei Zhai[1]

[1] China United Gas Turbine Technology Co., Ltd., Beijing, China
[2] China Automation Industry Chain Alliance (Beijing) Technology Industry Development Co., Ltd., Beijing, China

Abstract. With the development of digital and intelligent technology in industrial control, the safety and reliability of control and protection system is becoming increasingly prominent. As the Pearl of modern industry, heavy duty gas turbine is very important. The ongoing independent R&D work of UGTC (China United Gas Turbine Technology Co., Ltd.) has been highly concerned by the industry. As the nerve center system of gas turbine, whether the control and protection system can complete the expected function safely and reliably is also an important part of the independent R&D work of heavy-duty gas turbine. In this paper, combined with the independent research and development experience of nuclear power control and protection system in China, based on the functional safety certification requirements of IEC 61508 standard, the technical scheme of heavy-duty gas turbine control and protection system software V&V is discussed, and the relevant technical key points are put forward, which has a certain guiding significance for the design and commissioning of control and protection system of heavy-duty gas turbine.

Keywords: Heavy-duty gas turbine · Control and protection system · Software verification and validation

1 Introduction

Since the invention of BBC company in 1939, gas turbine has been widely used in power generation, pipeline power, ship power, locomotive power and other fields after more than 60 years of development. It is an important high-end technology equipment integrated with many technologies, and plays an important role in national defense, energy, transportation and other industrial sectors 1.

With the emergence of new technology of heavy-duty gas turbine and the improvement of market demand, its control system has gone through three stages: mechanical hydraulic control, analog electronic control and digital electronic control. Today, it has developed into a highly complex, distributed, multi redundant, nonlinear and multi-functional digital electronic control system, become a set of modern optical, mechanical, electrical, information and control technology as one of the high-tech products 1.

Y. Xu et al. (Eds.): SICPNPP 2020, LNEE 779, pp. 757–764, 2021.
https://doi.org/10.1007/978-981-16-3456-7_76

The independent R&D of heavy-duty gas turbine in China has entered a critical stage. As the nerve center system of gas turbine, whether the control and protection system can complete the expected function safely and reliably is one of the key factors for the success of heavy-duty gas turbine research and development.

Combined with the successful experience of independent research and development of control and protection system in China's nuclear power industry and the requirements of functional safety certification based on IEC 61508 standard, this paper discusses the technical scheme of software V&V (Verification and Validation, V&V) of control and protection system for heavy-duty gas turbine and puts forward the key technical points in the process of implementing software V&V, and provides technical guidance for the detailed design and system commissioning of the control and protection system of the subsequent heavy-duty gas turbine.

2 Difficulties in Control and Protection System of Heavy Duty Gas Turbine

Heavy duty gas turbine has the characteristics of complex process flow, fast dynamic process and strong nonlinear coupling. There are many technical difficulties in the design of its control and protection system, such as multiple control objectives, high target requirements, high control accuracy and large control scale. With the deepening application of digital, intelligent and other new technologies, the safety and reliability of its control and protection system has become increasingly prominent.

In order to reduce the accident risk caused by the failure of control and protection system, the gas turbine protection system must meet the functional safety requirements of IEC 61508 SIL3.

Siemens gas turbine protection system adopts AS620F (s5-95f/h) fault safety subsystem, France Alstom applies CE3500 triple redundant subsystem of ALSPA system for gas turbine control and protection, American GM also introduces Mark VI control and protection system, and Japan Mitsubishi Heavy Industry (MHI) uses DIASYS system for gas turbine control and protection in August 2013, all of which comply with IEC 61508 Sil3 functional safety requirements and certification [3].

In recent decades, domestic industrial control system products have also developed rapidly. The industrial control system independently developed by Chinese companies has achieved good application performance in coal, chemical and electric power industries, but it is very difficult to pass IEC 61508 SIL3 functional safety certification.

In China's nuclear power industry, due to the particularity of nuclear power safety, the FirmSys platform of nuclear power station protection system of CGN not only carries out software V&V according to IEEE 1012 integrity level 4, but also does the related work of IEC 61508 sil3 functional safety certification, and obtains some experience, Firmsys system has been well applied in Yangjiang 5, 6 units and Tianwan 5, 6 units.

The NUPAC system independently developed by SPIC has also carried out relevant work in accordance with IEEE 1012 integrity level 4 and IEC 61508 SIL3 functional safety certification, and will also be applied in the CAP1400 demonstration project in Shidao, Shandong Province.

In the above design and verification process, how to effectively implement software V&V is one of the key points and technical difficulties. Therefore, in the process of independent R&D of heavy-duty gas turbine control and protection system, it is very important to plan the software V&V scheme of control and protection system according to the requirements of regulations and standards.

3 Discussion on Key Points of Software V&V Scheme

Both the SIL level of IEC 61508 and the integrity level of IEEE 1012 are risk-based classification schemes.

According to the severity of the consequences of errors in function or system characteristics and the probability of these consequences, the SIL or integrity level of the system and software is generally divided into four levels, among which level 1 is the lowest and level 4 is the highest.

Software V&V process includes verification process and validation process.

The objective data provided by the verification process is used to prove whether the product meets the requirements of all activities in each stage, whether it meets the standards and specifications, and whether it successfully completes all activities and meets the conditions for starting subsequent activities.

Confirm the objective evidence provided by the process to prove whether the product meets the specified system requirements at the end of each phase and finally meets the expectation 4.

Based on the experience of nuclear power control and protection system software V&V engineering and combined with the standard requirements, the key points in the software V&V practice are as follows:

3.1 The Organizational Model of Maintaining Relative Independence

In the organizational model composed of design R&D team, manufacturing team, V&V team and expert team, the independence of each team should be maintained, with the emphasis on the independence of design R&D team and software V&V team. Independence is mainly reflected in three aspects: technical independence, management independence and financial independence:

1) technical independence
   Technology independence requires that the V&V team members should not include the R&D team members, and the V&V team should form an independent and systematic test plan. Technical independence is mainly through the independence and diversity of personnel, methods and tools to identify those subtle errors that are easy to be ignored by the development team.
2) managerial independence
   Independent management, on the one hand, means that the responsibility of the V&V team belongs to an independent management department. On the other hand, it means that the V&V team can independently choose the software and system for analysis and testing, select the technology used for test verification, customize the

test and V&V work plan, and submit all the software V&V test results and abnormal information to the management department.

3) financial independence
Financial independence means that the budget of V&V work is controlled by organizations other than R&D to prevent the influence of misappropriation of funds or adverse financial pressure.

As shown in Table 1, according to the above three forms of independence, V&V organization can be divided into five types: typical, modified, integrated, internal and embedded.

Table 1. Forms of V&V

V&V Form	Technical	Management	Financial
Classical	I	I	I
Modified	I	i	I
Integrated	i	I	I
Internal	i	i	i
Embedded	e	e	e

I: Rigorous independence; i: Conditional independence; e: Minimal independence

1) Classical V&V
The classical V&V organization form is usually in charge of an organization completely independent of the R&D team in terms of technology, management and finance. In the classical V&V, on the one hand, the V&V team should ensure the independence of the R&D team, on the other hand, it should establish a close working relationship with the development team, so as to ensure that the conclusions and suggestions of software V&V can be quickly integrated into the software development work. Generally, the classical V&V must be used for software verification of software integrity level 4.
2) Modified V&V
The modified V&V organization form is suitable for large-scale program verification, and its V&V team and R&D team belong to the same management organization. Under the same management structure, the efficiency of connection between V&V and R&D work is improved, but the independence of management is reduced. At the same time, the technical and financial independence of V&V is retained because the result report of V&V is submitted to the superior management. Generally, the modified V&V form is suitable for software verification of software integrity level 3.
3) Integrated V&V
The integrated V&V organization form is mainly used for fast feedback of V&V results. This form of financial and management is independent of the R&D team,

which can maximize the independence of V&V. In this form, the V&V team can work side by side with the R&D team, review the unpublished R&D samples in time, and provide V&V feedback in the process of R&D team's own inspection and review.

4) Internal V&V
The internal V&V organization form should not use the same personnel in the R&D team when the R&D team uses its internal members as the V&V team. The independence of technology, management and finance has been weakened. The main reason for the weakening of technical independence is that the internal V&V in the testing process is easy to ignore the mistakes in the development process because of adopting the same assumptions and development environment. The reason for the weakening of management independence is that the R&D team and the V&V team are under the same management organization, so the negative pressure of the software R&D team is likely to have a negative impact on the work of the V&V team.
5) Embedded V&V
Embedded V&V organization, V&V work using internal members of R&D team, should avoid V&V team members directly participating in R&D work. It focuses on the consistency of V&V process and development process. It is helpful to provide feedback of V&V results in the process of product development, but it will reduce the independence of V&V team in technology, management and finance.

3.2 Identify Software V&V Processes and Tasks

The "V-diagram" (see Fig. 1) model based on IEC 61508 includes the identification of V&V technology content in each stage and the determination of various technical conditions.

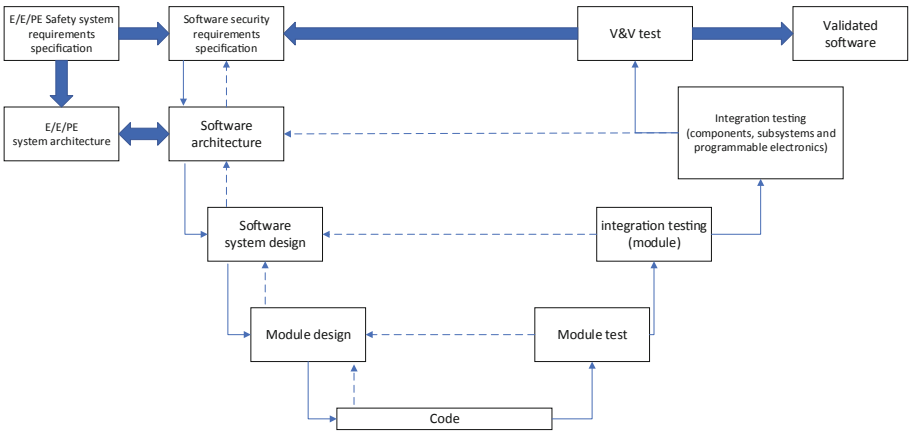

Fig. 1. Software V&V model

As shown in Fig. 1, software V&V work is carried out in phases according to the control and protection system development life cycle process defined by the project.

Software architecture design V&V mainly validates the software architecture design according to the software security requirements, and makes the system integration test plan;

Software system design V&V mainly verifies the software system design according to the software architecture design, and formulates the software integration test plan; Software module design V&V focuses on module design verification according to software system design, and makes module test plan; Software coding V&V mainly evaluates the conformity of software source code and related design documents through static or dynamic testing.

After that, software integration test, system integration test and system validation were carried out in turn. The parallel development of V&V work and design R&D work enables the V&V team to intervene in each stage of the system development life cycle process as soon as possible, find out the errors, defects and omissions of requirements and design in time, modify the requirements and design scheme as soon as possible, and avoid a lot of rework in the later stage, so as to greatly save manpower cost and guarantee the progress.

3.3 Selection of Test Methods and Verification Tools

As far as possible, the R&D team and V&V testing team should choose independent verification tools. Limited by the support environment and the cost of independent tools, there is a situation of sharing tools. For the shared testing tools, the software V&V team needs to confirm their reliability and scope of application, so as to ensure that the shared tools do not contain errors that may cover up the errors in the analyzed and tested software.

Therefore, V&V team should pay attention to the following points in the selection of test verification tools:

1) Modular development method should be adopted as far as possible to reduce the use of verification tools;
2) Independent research and development of relevant verification tools to minimize the procurement of foreign tools;
3) Purchase necessary foreign verified or approved tools in other industries.

3.4 Problem Handling Process

The work between R&D team and V&V team is an interactive workflow, so it needs a complete process of problem handling, document modification and submission.

As shown in Fig. 2 software V&V work problem processing flow chart. Generally, design documents (first edition) are prepared by R&D team and submitted to V&V team. For the problems found in the verification, the V&V team will put forward the problem sheet to the R&D team for confirmation. If the R&D team accepts the questionnaire and modifies it, the V&V team will conduct regression verification to confirm that the modification is correct and then proceed to the follow-up process. However, in the case that the R&D team does not accept the questionnaire, the V&V team and the R&D team negotiate to complete the problem confirmation. The treatment of controversial issues

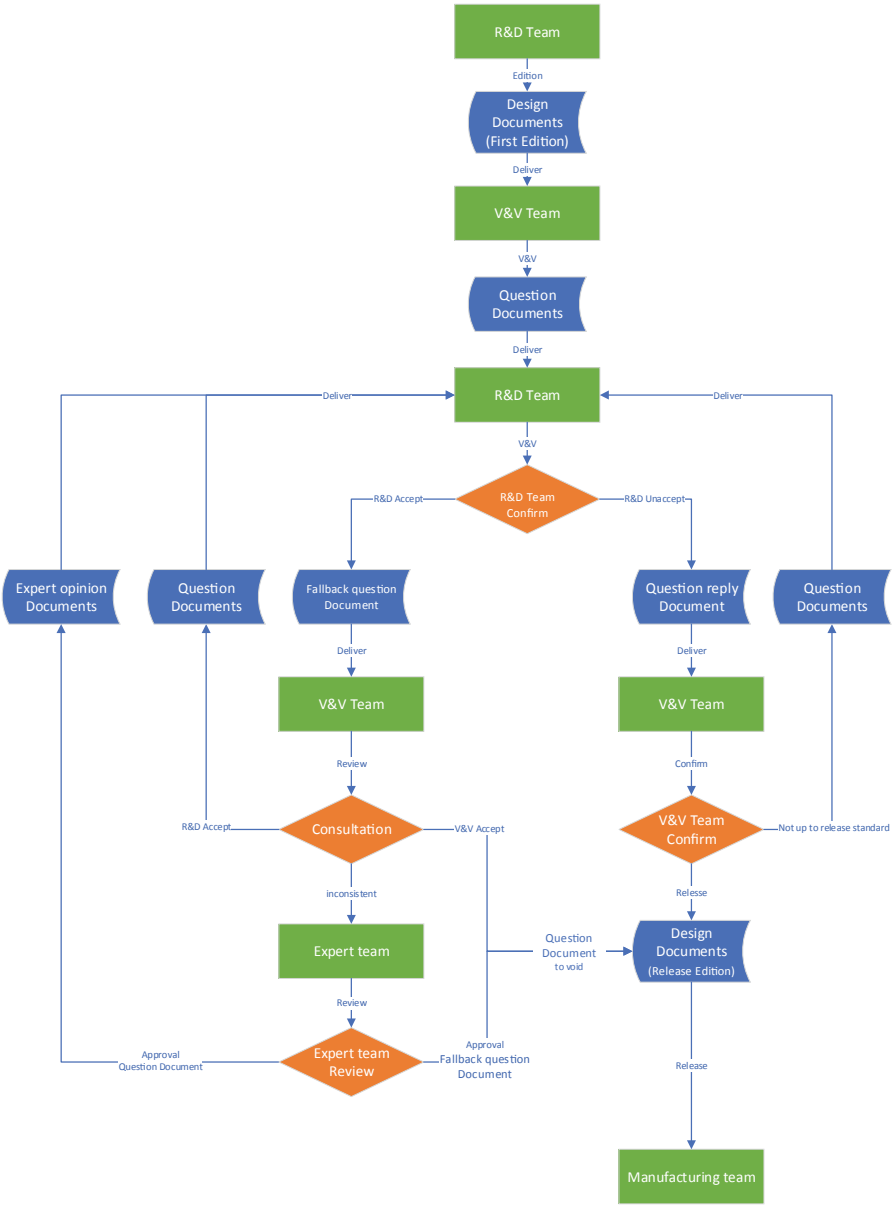

Fig. 2. Software V&V work flow chart

will be decided by the expert team, and attention should be paid to the classification of problem levels at the beginning. Problems of different levels are generally determined according to the degree of harm. The classification of problem levels has very important practical significance for FMEA analysis at the follow-up system level.

4 Conclusion and Prospect

The independent R&D of China's reburning gas turbine has entered a critical stage. With the gradual determination of process system, the demand of control and protection system will be determined. With the further deepening of the design, installation and debugging related work will also enter a critical stage. As the nerve center system of gas turbine, whether the control and protection system can complete the expected function safely and reliably is also an important part of the independent R&D work of heavy-duty gas turbine. Referring to the successful experience of independent research and development of control and protection system in China's nuclear power industry, the technical scheme of heavy-duty gas turbine control and protection system software V&V is implemented based on the functional safety certification requirements of IEC 61508 standard, which has a good guiding significance for the detailed design and system debugging of the follow-up heavy-duty gas turbine control and protection system.

References

1. Saite, W.: Review on the research of application of gas turbine. Light Ind. Sci. Technol. **35**(12), 52–54 (2019)
2. Shangming, L., Ai, H., Hongde, J.: Development trend of heavy-duty gas turbine control technology. Therm. Turb. **42**(04), 217–224 (2013)
3. Feiyang, H.: Development of heavy duty gas turbine control technology. Sci. Technol. Inf. **15**(10), 43–44 (2017)
4. Zekan, C., Shuaike, G.: Verification and validation of non-1E DCS software in digital nuclear power plant. Tech. Autom. Appl. **39**(10), 61–66 (2020)