# A Summary of the Guidelines on the Evaluation of V&V Tools for Safety Digital I&C Software in Nuclear Power Plant Systems

**Nan Wang, Lingpo Li, Ruidong Dai and Chun Guo**

**Abstract** With the rapid development of the digitalized instrumentation and control (I&C) systems, computer-based and software-driven systems have been employed in nuclear power plant on a large scale. Automated tools take a crucial role in the software verification and validation (V&V) process. However, defects in the tools may bring uncertainty, risk, and even failures to the safety software if the tools are not well designed, carefully developed, effectively tested, and appropriately used. Therefore, it is critical that automated tools should be evaluated and tested for the reliability, accountability, and feasibility before they are used in the software V&V process. However, there is no widely accepted method to evaluate the tools. Many methods for tool evaluation have been proposed by different organization, including nuclear industry and other high reliability industry. This study is a survey of the current practice and standards related to the evaluation of tools for safety-related digital Instrumentation and Control (I&C) software for nuclear power plants. Standards and documents from organizations such as IEEE, IAEA, and NRC Regulations are collected and analyzed in this paper. By summarizing and analyzing the related standards and practice, this study intends to explain what should be done for the evaluation of the tools, which may be used in the self-reliance process of nuclear industry in China.

**Keywords** Digital I&C · V&V · Software tools · Standards · Regulatory guidance

## 1 Introduction

With the advanced nuclear power reactors under development, the demand for safety I&C system is urgent. The tools used for the evaluation of the developed product should have high reliability and accountability. In terms of verification and

N. Wang (✉) · L. Li · R. Dai · C. Guo
State Nuclear Power Automation System Company, Shanghai, China
e-mail: wangnanb@snpas.com.cn

© Springer Science+Business Media Singapore 2017

H. Jiang (ed.), *Proceedings of The 20th Pacific Basin Nuclear Conference*,
DOI 10.1007/978-981-10-2317-0_2

validation process, automated software tools are frequently used. Uncertainty and even risks should be controlled in an acceptable level so that tools will not affect the feasibility and reliability of the whole system.

This paper does a survey of the current regulations, guides, and standards that are relevant to the V&V process. A summary of the information related to the software tools is listed. Based on the information, a detailed guideline to the V&V work is pictured.

## 2 Discussion and Survey Summary

### *2.1 RG 1.152*

Regulatory Guide (RG) 1.152, Revision 3 [1], provides a method for "promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems of nuclear power plants", which is accepted by NRC. This regulatory guide takes hardware, software, firmware, and interfaces into account based on waterfall life cycle.

Section 2.2 describes the requirement of predeveloped software and systems. It is emphasized that unnecessary or extra requirement and codes should be prohibited.

Section 2.3 describes the software tool requirement of design phase. Predeveloped software shall guarantee the safety of the operating environment. Special measurements should be taken if unwanted features are introduced.

Section 2.4 describes the software tool requirement of implementation phase. Due to the fact that most of the COTS software is confidential, reviews cannot be conducted directly because of uncertainty. Developers are required to ensure the COTS software will not threaten the operating environment.

The conclusion reached from the (RG) 1.152, Revision 3 [1], is that development and operating environment must be ensured, for the sake of preventing unnecessary and unauthorized code. Besides, the review of COTS and predeveloped software should be considered carefully.

### *2.2 RG 1.168*

RG 1.168, Revision 2 [2], provides a method for software V&V and review, which is accepted by NRC. There is not much information related to software tools.

Section C 3 requires that if the product will be introduced in a safety-related system, the licensee shall be responsible for assuring that the V&V and software

quality meet the NRC's requirements for reliability. The independence of V&V software tools should comply with regulations and laws.

Section C.4 requires that the acceptance of preexisting software shall be based on RG 1.152.

Section C.6 describes the requirement of safety-related system software tools. "V&V tasks of witnessing, reviewing, and testing are not required for software tools, provided the software that is produced using these tools is subject to V&V activity that will detect flaws introduced by the tools."

## *2.3 RG 1.169*

RG 1.169, Revision 1 [3], discusses the method of configuration management, which is accepted by NRC.

Section C.6 requires that configuration items or controlled documents shall include all the supportive software during development phase and codes used during testing.

Section C.7 requires commercial software dedication for safety-related systems shall comply with the recommendation of EPRI TR-106439.

Section C.8 requires that all the software that is used during development phase shall be managed according to IEEE 7-4.3.2-2003. Besides, software tools during development phase should be treated as a configuration item.

## *2.4 RG 1.170*

RG 1.170, Revision 1 [4], discusses the test documentation of safety-related digital computer software in a nuclear power plant. It requires that the minimum documentation package shall include all the elements that are essential for completing the task, including environmental conditions, special controls, equipment, tools and instrumentation.

## *2.5 RG 1.172*

RG 1.172, Revision 1 [5], discusses the software requirement specification of the digital I&C system in a nuclear power plant. If representation tools are used to express the requirements, the traceability between the representations and natural language descriptions of the software requirements needs to be maintained.

## 2.6 RG 1.173

RG 1.173, Revision 1 [6], discusses the process of software life cycle. This guide has little relevance with software tools. It mainly focuses on the acceptable process of COTS software evaluation.

## 2.7 DI&C-06

DI&C-06 requires dedicating COTS and predeveloped software tools for safety-related systems based on EPRI TR-106439.

## 2.8 NUREG-0800

NUREG-0800 [7] BTP 7-14 requires that software tools shall be reviewed according to their rigidity. Methods, techniques, and tools shall be verified to an acceptable degree.

NUREG-0800 Appendix 7.1-D requires that the system shall meet single-failure criterion. Software tools shall not violate single-failure criterion, especially compliers and linkers. Section 5.3 of this appendix discusses the usage of software tools. Review of software tools shall comply with the content in IEEE 7-4.3.2-2003 and IEC 60880-2. "If, however, it cannot be demonstrated that defects not detected by software tools or introduced by software tool will be detected by verification and validation (V&V) activities, the software tool should be designed as safety-related software itself, with all the attendant regulatory requirements for safety software."

## 2.9 NUREG/CR-6421

NUREG/CR-6421 [8] proposes an approval process for COTS software employed in nuclear power plant safety systems. Section 1.3 states that the system software tools are important for safety. Therefore, they shall be classified as critical software tools. The safety category classification of COTS software is category A, B, C, or unclassified.

## 2.10 IEEE Std 7-4.3.2

IEEE Std 7-4.3.2-2010 [9] Sect. 5.3.2 discusses the usage of software tools, which contains two criteria. The first one is that the output of the software needs to be verified and validated based on the same safety degree of the software. The second one is that development and commercial dedication shall be conducted according to quality assurance requirement in 10 CFR 50 Appendix B.

## 2.11 IEEE Std 603-2009

IEEE Std 603-2009 [10] provides the minimum functional design for the safety system in a nuclear power plant. Two important proposed concepts are the isolation between safety and non-safety systems and the single-failure criterion. It also accounts common cause failure, which is defined as "loss of function to multiple structures, systems, or components due to a shared root cause". Software tools evaluation should take single-failure criterion and common cause failure into account.

## 2.12 IEEE Std 1012

IEEE Std 1012 [11] extends the definition description of the software tool by different revisions. IEEE Std 1012-2012 requires that "If the tool cannot be verified and validated, then the output of the tool shall be subject to the same level of V&V as the software element".

## 2.13 IEEE Std 14102

IEEE Std 14102-2010 [12] defines the process and features of CASE tool selection. This standard can be used during the process of software tools technical evaluation and selection. The process of tool selection includes preparation, definition, evaluation, and selection. The subsequent documentation can demonstrate the quality of selected tools.

### *2.14 IAEA NS-G-1.1*

IAEA NS-G-1.1 [13] describes the planning, documentation, selection, and qualification of software tools. This guide considers all categories of software: preexisting software (e.g., an operating system), software developed for the project (testing software tools).

Section 3 requires that software based on computer systems shall hold diversity and variety. Software tools shall commensurate within different phases. Based on the function in the development phase and the safety-related requirement, software tools need to be dedicated accordingly.

Section 10 [13] focuses on the software verification and validation. Software verification and validation tools will not introduce defects to the system. However, it also may not detect defects. For tools including V&V tools, it is necessary to have adequate safety features to ensure overall safety. During the V&V process, test operators shall keep adequate records (including tools, input, setup etc.) in order to demonstrate that the process of V&V tests can be repeated.

## 3 Conclusions

Regarding to software tools, guides and standards surveyed in this paper directs that

1. Software tool verification and validation shall be conducted based on application methods and functions to assure the accuracy.
2. Configuration management is essential.
3. Commercial software that is directly used in nuclear power plants shall conduct the CGI dedication.

Detailed explanation is as following (e.g., test signal generating devices):

1. According to IEEE 1012-2012, it is regarded as tool without codes. Therefore, verification needs to be done to ensure the correctness of the function.
2. According to IAEA NS-G-1.1, it is regarded as a V&V tool. It is required to figure out the function and effect on the environment and then start the evaluation task accordingly.
3. According to IEEE 7-4.3.2-2003, a V&V program needs to be developed to demonstrate that the tool can be function correctly as the requirement states.
4. According to IAEA NS-G-1.1, based on testing requirement, clear and adequate records are demanded, as well as calibration and standardization of the tool periodically.
5. In addition, it shall comply with the basic quality assurance requirement. Development phase documentation of the tool is also required.

## References

1. Regulatory Guide 1.152, Revison 3
2. Regulatory Guide 1.168, Revison 2
3. Regulatory Guide 1.169, Revison 1
4. Regulatory Guide 1.170, Revison 1
5. Regulatory Guide 1.172, Revison 1
6. Regulatory Guide 1.173, Revison 1
7. NUREG-0800
8. NUREG/CR-6421
9. IEEE Std 7-4.3.2-2010
10. IEEE Std 603-2009
11. IEEE Std 1012-2012
12. IEEE Std 14102-2010
13. IAEA NS-G-1.1

http://www.springer.com/978-981-10-2316-3

Proceedings of The 20th Pacific Basin Nuclear Conference
Volume 2
Jiang, H. (Ed.)
2017, XIV, 936 p. 490 illus., Softcover
ISBN: 978-981-10-2316-3