Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, November 2-3, 2006

A Development of Software V&V Criteria for SMART MMIS

Yong Suk Suh,[a] Heui Youn Park,[a] Hyeon Soo Kim,[b] Ki Sung Son,[c] Se Hyung Jung [c]
a I&C and HF Div., KAERI, 150 Dukjin-dong, Yuseong-gu, Daejon, Korea, 305-353, yssuh@kaeri.re.kr
b Dept. of Computer Sci. and Eng., Chungnam Nat'l Univ., 220 Gung-dong, Yuseong-gu, Daejon, Korea, 305-764
c Control Tech. Research Inst., SEC Co., Ltd.,974-1 Goyeon-ri Woongchon-myon, Ulju-gun, Ulsan, Korea, 689-871

1. Introduction

The Pre-Project Study (PPS) for the construction of SMART (System-integrated Modular Advanced ReacTor), which is a feasibility study on its construction, is being performed by KAERI. The MMIS (Man-Machine Interface System) is one of the sub-studies of the PPS. Among several items of the MMIS study, the software V&V (Verification and Validation) is being studied by the authors of this paper. The software V&V is one of the major factors to achieve the license of the MMIS from the nuclear regulatory authority. For this achievement, the V&V plan and the results of the V&V activities shall be submitted to the authority. In order to create the V&V plan, we reviewed domestic and US nuclear laws, regulations, and industrial standards. These references describe why the V&V is required and what the V&V does. However, these references provide plenty of information with different points of view. Therefore it is necessary to summarize the information. As 10CFR50 does, we applied the generation of criteria to the summarization. Appendix A to 10CFR50 describes 64 general design criteria and Appendix B 18 quality assurance criteria. The criteria provide top-tier and minimum requirements for a water-cooled nuclear power. So, we conclude that the creation of the software V&V criteria is the best way for the summarization. The V&V criteria will then be used as criteria in producing the V&V plan and the relevant V&V activities for the SMART MMIS. The criteria are presented in the following section.

2. The Criteria

First, we reviewed the domestic nuclear laws [1], regulations [2], [3]; industrial codes [4], [5], [6]; and information of the regulatory guides [7], [8], [9]; and USA nuclear laws [10], [11], [12]; industrial standards [13]-[20]; information of the regulatory guides [21]-[26] in order to create the V&V criteria.

As a result of the review, 16 criteria were derived and the criteria were categorized in terms of the overall requirements, plan, activity, independence, use of software tool, documentation, and management requirements. These are described in the following subsections.

2.1 Overall Requirements

Criterion – 1: In order to perform the V&V, the plan shall be established and documented, the activities shall be performed as described in the plan, and evidence of the activities shall be shown and documented.

Criterion – 2: The V&V should ensure not only that the software satisfies the requirements imposed on the software but also that unintended functions are not implemented in the software. For this, the V&V shall elicit quality characteristics which are not limited to correctness, completeness, consistency, etc, from the software requirements and identify them in the software.

Criterion – 3: The V&V shall be performed in parallel with a software development life cycle which consists of several phases such as a requirement analysis, design, implementation, validation, installation, operation and maintenance. Each phase of the cycle shall not proceed to the next phase until all the V&V activities imposed on the phase are completely finished.

Criterion – 4: When a software defect is detected during the V&V activity, the detection activity shall continue until it is assured that all the subsequent defects do not exist.

Criterion – 5: When a software is required to rework as a result of the V&V, the V&V shall ensure that the software is correctly reworked as required. Whenever a baseline software is changed, the V&V shall ensure that the software is correctly changed, unintended functions are not added, and the software does not interfere with the performance of other software.

2.2 Plan Requirements

Criterion – 6: The V&V plan shall identify inputs to the V&V, activities and methods of the V&V, and outputs from the V&V. The plan shall encompass not only software but also interfaces to hardware and interfaces to externals such as users, environments, and systems.

Criterion – 7: The V&V plan shall define the criticality of a software, determine the level of V&V activities corresponding to the criticality, and describe the procedures of the activities.

Criterion – 8: The V&V plan shall include the V&V reporting process and administrative requirements that support the V&V activities.

2.3 Activity Requirements

Criterion – 9: The V&V activity shall consist of at least a planning task, testing, reporting, documenting, and a logging task.

Criterion – 10: The software testing shall include module testing and system testing. The module testing shall test not only a module but also an integration of modules. The system testing shall include testing of the final integrated hardware, software, firmware, and interfaces. The software testing method shall include static testing and dynamic testing. The static testing shall include analysis, evaluation, and review. The dynamic testing shall include white-box testing and black-box testing. The testing shall be planned, designed, procedurally executed, reported in time, documented, and logged.

2.4 Independence Requirements

Criterion – 11: The V&V shall be performed by individuals and groups who did not developed the original design. When the V&V is performed by the independent V&V team, at least a technical, managerial, and financial independency shall be guaranteed to the team.

2.5 Use of Software Tool Requirements

Criterion – 12: Prior to using a software tool for the V&V, it shall be evaluated to ensure that it conforms to the requirements of the V&V. Although the V&V is finished with the use of a software tool, the final result of the tool shall be verified manually.

2.6 Documentation Requirements

Criterion – 13: The V&V plan, anomaly report, and summary report shall be documented as a minimum. Only the documents which are approved by the project manager shall be effective. The configuration of the approved documents shall be controlled.

2.7 Management Requirements

Criterion – 14: The software which is submitted to the V&V team shall be formally approved by the project manager.

Criterion – 15: The V&V plan and activities shall be controlled and managed so as to ensure that the risks and contingencies for the V&V are well controlled.

Criterion – 16: The V&V activities shall interact with the activities of the software development team, quality assurance, configuration management, safety analysis, and the project management team. Especially for the defense against a software common cause failure, the V&V activities shall be performed in conjunction with the safety analysis team.

3. Conclusion

The development of software V&V criteria was required by the PPS of SMART MMIS. To this end, this paper presents 16 software V&V criteria which are derived from domestic and USA nuclear laws, industrial standards, and regulatory guides. They will be used as the top-tier requirements and acceptance criteria in developing the V&V plan and V&V activities for the SMART MMIS. Even if the criteria are not for general purpose, this paper recommends that the nuclear regulatory authority uses them as criteria to accept a V&V plan and relevant V&V activities for nuclear power plants.

REFERENCES

[1] Atomic Energy Act (AEA), Chapter 4, “Construction and operation of nuclear power reactors and related facilities”, ROK, 2005.

[2] Enforcement Regulation of the AEA, Number 31, “Regulations on Technical Standards for Nuclear Reactor Facilities, etc.”, MOST, ROK, 2006.

[3] Notice of the MOST, Number 2001-47, “Detailed Requirements for Quality Assurance of Nuclear Reactor Facilities”, MOST, ROK, 2001.

[4] KEPIC QAP-1, “Nuclear Quality Assurance”, KEA, ROK, 2000.

[5] KEPIC QAP-2 II.7, “Quality Assurance for Computer Software for Nuclear Facilities”, KEA, ROK, 2000.

[6] KEPIC ENB 6370, “Safety System Digital Computer”, KEA, ROK, 2000.

[7] KINS/RR-033, “Development of Regulation Technologies for Software Verification and Validation of I&C Systems Important to Safety in NPPs”, KINS, ROK, 2000.

[8] KINS/RR-106, “Development of Safety Requirements and Guides for Digital-Based I&C Systems Important to Safety in Nuclear Power Plants”, KINS, ROK, 2002.

[9] KINS-G-001, Section 7, “Instrumentation and Controls”, SRG Rev.02, KINS, ROK, 1999.

[10] 10CFR50.55a, “Codes and Standards”, US NRC, 2000.

[11] 10CFR50 App. A, "General Design Criteria for Nuclear Power Plants", US NRC, 2000.

[12] 10CFR50 App. B, "Quality Assurance Program", US NRC, 1995.

[13] IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations", 2003.

[14] IEEE Std 610.12, "IEEE Standard Glossary of Software Engineering Terminology", 1990.

[15] IEEE Std 730, "IEEE Standard for Software Quality Assurance Plans", 1998.

[16] IEEE Std 829, "IEEE Standard for Software Test Documentation", 1998.

[17] IEEE Std 1008, "IEEE Standard for Software Unit Testing", 1987.

[18] IEEE Std 1012, "IEEE Standard for Software Verification and Validation", 1998.

[19] IEEE Std 1028, "IEEE Standard for Software Reviews", 1997.

[20] IEEE Std 1074, "IEEE Standard for Developing Software Life Cycle Process", 1997.

[21] RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants", US NRC, 2006.

[22] RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", US NRC, 2004.

[23] RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", US NRC, 1997.

[24] RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", US NRC, 1997.

[25] NUREG-0800, Section 7.0, “Instrumentation and Controls", US NRC, Rev. 4, 1997.

[26] SECY-93-087, II.Q, “.Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems”, US NRC, 1993.