Comparison of the Safety Critical Software V&V Requirements for the Research Reactor Instrumentation and Control System

Sungmoon Joo*, Yong-Suk Suh, Cheol Park
Korea Atomic Energy Research Institute, Daedeok-daero 989-111, Yuseong-gu, Daejeon, Korea
**Corresponding author: smjoo@kaeri.re.kr*

1. Introduction

For modern, digital instrumentation and control (I&C) systems of research reactors, effective verification and validation (V&V) are key activities for the qualification of safety-critical software. V&V are also essential for the approval from regulatory bodies. As standards define or recommend consolidated engineering practices, methods, or criteria, V&V activities for software qualification are not exceptional.

Within a standards framework, usually, the processes for the qualification of safety-critical software are well-established such that the safety is maximized while minimizing the compromises in software quality, safety, and reliability.

When, however, multiple standards frameworks are involved in a research reactor project, it is difficult for equipment vendors to implement appropriate V&V activities as there is no unified view on this cross-standards-framework qualification issue yet.

This study was motivated by a research reactor project where the owner of the project and the equipment vendors are from two different standards frameworks. This paper reviews two major standards frameworks - NRC-IEEE and IAEA-IEC - and the software classification schemes as a background, then discuss the V&V issue. The purpose of this paper is by no means to solve the cross-standards-framework qualification issue, but, rather, is to remind the stakeholders of research reactor projects.

2. Standards and Framework

Standards must be established such that the characteristics of the domain in which they are applied are properly accounted for. A standards framework for certain domain is the systematic representation of these domain characteristics.

There are two major and widely adopted international standards frameworks for nuclear reactor instrumentation and control (I&C) software, NRC-IEEE and IAEA-IEC [11,12]. The top level IEEE standard for nuclear power plant (NPP) safety systems is part of US Nuclear Regulatory Commission (NRC) regulations, and IEC takes IAEA safety standards, primarily NS-G-1.3, as the basis for their standards. Thus, the NRC requirements and IAEA safety standards are important framework elements for IEEE and IEC, respectively. Table I summarizes the two frameworks for nuclear I&C software.

IEC standards tend to be more broadly applicable, but less specific than IEEE standards. In terms of safety principles, safety shall be met through a thorough engineering and the qualification is assured indirectly in IEC standards. These differences can partly be attributed to the philosophies the two standards are based upon; IEC standards are more about "Goals and How to do", while IEEE standards are focusing on "What to do."

Table I: Major Standards Frameworks for I&C Software

	NRC-IEEE	IAEA-IEC
Code	10CFR50	NS-G-1.3 (I&C Safety Guide)
	IEEE 603 (Safety system) / RG 1.153	
	IEEE 7-4.3.2 (General guide) / RG 1.152	NS-G-1.1 (Software Safety Guide)
		IEC 61513 (General requirement)
Regulatory Guide	SRP-NUREG-0800	IEC 61226 (Classification)
	RG 1.168, RG 1.169, RG 1.170, RG 1.171, RG 1.172, RG 1.173	
Industrial Code & Std.	EEE 828 (CM plan) IEEE 829 (Test documentation) IEEE 830 (Requirement spec.) IEEE 1008 (Unit test) IEEE 1012 (V&V) IEEE 1016 (Design spec.) IEEE 1028 (Review & Audit) IEIEEE 1042 (CM guideline) EE 1074 (Life cycle process)	IEC 60880 (Category A S/W) IEC 62138 (Category B&C S/W)

3. Safety Classification

3.1 Function, System and Equipment Classification

The classification of functions, systems and equipment (FSE) into safety classes is an important part of a research reactor project. The classification is intended to ensure that each FSE is given the attention or is allocated the resource it requires, based on its significance with regard to safety; all FSEs for PIEs (Postulated Initiating Events) are assigned to the highest safety class, while less important FSEs are allocated to lower safety classes. Thus, the safety classification can be used as a means to implement the graded approach for resource allocation.

Table II provides an overview of the different classification schemes implemented in different regulatory regimes and standards. In each safety classification schemes, technical and design requirements differ for each safety class; FSEs are designed such that their quality and reliability are in accordance with their safety class; following the principle, lower safety class FSEs have less strict requirements while more strict requirements are imposed on FSEs belonging to higher safety class.

Table II: I&C SFE Safety Classification

Country/Organization		Safety Classification of I&C Functions and Systems			
IAEA (NS-G-1.3)		Systems Important to Safety			Systems Not Important to Safety
		Safety	Safety-related		
IAEA (SSG-30)	Function Category	Safety Category 1	Safety Category 2	Safety Category 3	
	System Class	Safety Class 1	Safety Class 2	Safety Class 3	
IEC 61226	Function Category	Category A	Category B	Category C	Unclassified
	System Class	Class 1	Class 2	Class 3	
USA/IEEE		Systems Important to Safety			Non-Nuclear Safety
		Safety-related/1E	(not specified)		
Korea		IC-I	IC-II	IC-III	

3.2 Software Classification

Similar to SFE classification, software classification schemes are required for the qualification with graded approach. The level of software verification and validation (V&V) effort is usually determined in accordance with the software safety classification level. (Table III).

The IEEE Std. 1012-2004 adopts software integrity level (SIL) system, SIL 4 being the highest and SIL 1 the lowest. The minimum V&V tasks are determined by SIL. The SIL is a range of values that represent characteristics that define the importance of the software such as software complexity, criticality, and safety level. For SIL 4, software element must execute correctly otherwise catastrophic consequences (i.e. loss of life or system, extensive economic or social loss) will occur and no mitigation is possible.

The IEC 61226 classifies the system's function into four categories: Category A, B, C, and Unclassified. The classification is based on the importance for safety, which is assessed by the consequence of its failure; Category A is assigned to functions which play a critical role in the achievement or maintenance of nuclear reactor safety, while Category C is assigned to functions with less critical role. I&C functions with no direct safety role are assigned to unclassified category

Table III: I&C Software Safety Classification

Organization/Country	I&C Software Safety Classification			
IEC 61226	Category A	Category B	Category C	Unclassified
IEEE 1012	Software Integrity Level 4	Software Integrity Level 3	Software Integrity Level 2	Software Integrity Level 1
Korea	Safety-critical (SC)	Important to Safety (ITS)		Non-safety (NS)

4. V&V requirements for Safety-critical Software

When developing safety-critical software it is imperative to have software development practices which incorporate effective V&V activities. Within the two standards frameworks, there are several standards for the production of safety-critical software for nuclear I&C systems (Table I). These include IEC 60880, IEEE 7-4.3.2, and IEEE 1012 [6,7].

IEC 60880 describes the European standards for the qualification of the software for nuclear power generating stations. More specifically, IEC 60880 outlines the Category A software development methods. Rather than specifying particular techniques, IEC 60880 states the requirements on the product; it is up to the developer (i.e. vendor) to meet those requirements using whatever methods they considers suitable; the effects that particular methods are expected to achieve are described in an appendix to IEC 60880.

IEC 60880 describes 1. Independence of the verification; 2. Verification plan; 3. Design verification; 4. Implementation verification (with both general purpose and application-oriented languages and respective test reports); 5. Configuration of pre-developed software.

On the other hand, IEEE 7-4.3.2 provides general guidelines which recommend choosing a combination of the following V&V activities: independent reviews, independent witnessing, inspection, analysis, and testing. Some of these activities may be performed by developers, but independent reviews must be performed. IEEE 1012 contains details of V&V activities: 1. Software V&V processes: management, acquisition, supply, development, operation, maintenance; 2. Software V&V reporting, administration and documentation; 3. Detailing a software V&V plan outline [8].

V&V activities are essential in the software development lifecycle. While V&V play a key role in software development, there is a level of ambiguity in the use of these terms, which add another layer of difficulty in cross-standards-framework issue. This is evident from the difference in definition of these terms in literatures [1].

As mentioned earlier, the IEEE and IEC standards take philosophically different approaches to V&V. IEC 60880 expresses objectives to reach (i.e. Goals & How to do) whereas IEEE 1012 details activities to perform to reach these objectives (i.e. What to do). Thus, reviewing a design developed using IEEE 1012 against criteria based on the guidance of IEC 60880 is problematic and vice versa. Even though the two frameworks are solid and sound on their own, differences in detail can cause considerable complexity and extra expense for equipment vendors, project owners and regulatory bodies. One thing to note is that the extra effort may not make no major improvement in safety.

5. Concluding Remarks

There are two major standards frameworks for safety-critical software development in nuclear industry. Unfortunately different safety classifications for software and thus different requirements for qualification are in place. What makes things worse is that (i) there are ambiguities in the standards and rooms

for each stakeholders' interpretation, and (ii) there is no one-to-one mapping between the associated V&V methods and activities. These may put the stakeholders of research reactor projects in trouble.

Even though efforts have been made to resolve this issue such as standard harmonization [5], there seems to be a long way to go. For the time being, the stakeholders of research reactor projects reside in different standards frameworks need to (i) make efforts to understand other standards frameworks, and (ii) consider realistic course of actions to make progress in their nuclear project while minimizing compromises in safety, instead of adhering to their own original standards frameworks.

Acknowledgements

This work was supported by the National Research Foundation of Korea grant funded by the Ministry of Science, ICT and Future Planning (MSIP) (Grant Code: 2012M2C1A1026912).

REFERENCES

[1] International Atomic Energy Agency, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007).
[2] International Electrotechnical Commission, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Rep. IEC 61508, IEC, Geneva (2010).
[3] International Electrotechnical Commission, Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - General Requirements for Systems, Rep. IEC 61513, IEC, Geneva (2003).
[4] International Electrotechnical Commission, Functional Safety - Safety Instrumented Systems for the Process Industry Sector, Rep. IEC 61511, IEC, Geneva (2003).
[5] International Atomic Energy Agency, Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1327, IAEA, Vienna (2002).
[6] International Electrotechnical Commission, Nuclear Power Plants - Instrumentation and Control Systems Important to Safety – Software aspects for computer-based systems performing category A functions, Rep. IEC 60880, IEC, Geneva (2006).
[7] Institute of Electrical and Electronics Engineers, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Standard 7-4.3.2-2004, IEEE, New York (2004).
[8] Institute of Electrical and Electronics Engineers, IEEE Standard for Software Verification and Validation, IEEE Standard 1012, IEEE, New York (1998).
[9] International Atomic Energy Agency, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, IAEA Technical Reports Series No. 384, IAEA, Vienna, (1999).
[11] Core knowledge on instrumentation and control systems in nuclear power plants, IAEA Nuclear Energy Series, No. NP-T-3.12, 2011
[12] Safety Classification for I&C Systems in Nuclear Power Plants-Current Status & Difficulties, World Nuclear Association, Report No. 2015/008, Sep. 2015