Developing Digital Instrumentation and Control System for Experimental Power Reactor by Following IEEE Std 1012-2004 to be Verified and Validated

Restu Maerani, Saharudin, Sudarno, Sigit Santoso, Deswandri, Syaful Bakhri, Jae-Cheon Jung

1 Center for Nuclear Reactor Technology and Safety, National Nuclear Energy Agency of Indonesia (BATAN), Kawasan Puspiptek Serpong Gd. 80 Tangerang Selatan 15310, Indonesia
2 Teknik Elektro, Institut Teknologi Indonesia (ITI), Jl. Raya Puspiptek Serpong Tangerang Selatan 15310, Indonesia
3 Department of Nuclear Power Plant Engineering, KEPCO International Nuclear Graduate School, 1456-1, Shinam-ri, Seosaeng-myeon, Ulju-gun, Ulsan, 689-882, Republic of Korea

maerani@batan.go.id

Abstract. We will develop the Experimental Power Reactor of Indonesia (RDE), by adopting the HTR-10 type from Tsinghua University-China. The Instrumentation and Control (I&C) for RDE will developed with digital system technology which in the development process will have verification, validation, design and implementation, reviews, and audits for digital computer software activities. Software design for I&C system of Nuclear Power Plant (NPP) should be started by developing software requirement specification (SRS) to meet the requirement that systems and components should be designed, fabricated, erected, tested, and inspected. In the regulatory structure of developing nuclear power plant in Indonesia, BAPETEN also concern for the design development of important to safety with computer based system for nuclear power plant (NPP) by PERKA BAPETEN No.6 in 2012. Since BAPETEN did not state which standards should be use, we can refer to the standards that are commonly used globally. IEEE Std 1012™-2004 is recommended by the latest US. Nuclear Regulatory Commission Guide 1.168 in 2013 about verification, validation, reviews, and audits for digital computer software used in safety systems of NPP. This guide also recommends IEEE Std 279, “Criteria for Protection Systems for Nuclear Power Generating Stations,” or in IEEE Std 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations. In this research we will examine the recommendation activity that should be follow to meet the requirement of the regulatory body which is also covered in IEEE Std 1012-2004. Developing traceability analysis in the first activity will help the designer to trace the requirement to meet the design criteria and reach the effectiveness and performance of the I&C system. By tracing from the top tier recommendation, it will help the development I&C system of RDE to be verified and validate as the design criteria for HTR-10

Keywords: Software Requirement Specification, Verification, validation, requirements traceability, I&C system
1. Introduction
Indonesia had develop experiment power reactor which is a HTR-10 type. As a generation 4 of nuclear energy system, BATAN as the Nuclear Energy Agency in Indonesia chose this type because High Temperature Reactor-10 (HTR-10) is a Pebble Bed Reactor (PBR) type technology with very safe considerations, functions for cogeneration, has a fuel flexibility, has been tested, competitive prices, multipurpose, can be developed in all regions of Indonesia according to their needs, and to meet electricity supply needs.

The main concern of developing I&C system in HTR-10 reactor is to focus on instrumentation that works in high temperature environments, that is why for the HTR-10 I&C system should be develop by following technology which is modern instrumentation architecture for HTGRs[1]. The Instrumentation and control (I&C) system shall be functioned to monitor variables and system in normal operation, accident condition or to monitor any cause of accident, consequently I&C should be developed using computer-based system [2]. To develop a high proven technology, development of I&C system for this reactor should follow the right regulatory guide and use the right standards from the recommendation of regulatory commission.

From the Standard Review Plan (SRP) Appendix 7.1 Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety, has been stated that the acceptance criteria for I&C system has four category which is: criteria for protection system for NPP generating stations from the ANSI/ IEEE Std 279, general design criteria (GDC) of 10 Code of Federal Regulations (CFR) Appendix A, regulatory guides to follow the code and standards, and Branch Technical Position (BTP) [3]. Branch Technical Position (BTP) 7-14 guidance on software reviews for digital computer-based Instrumentation and control system review, explain that it is necessary to prepare plans for controlling software development activities, since this experimental power reactor will be developed using computer-based system [4].

The standard from IEEE Std 1012-2004 is recommended by regulatory guide 1.168 in 2013 about verification, validation, reviews, and audits for digital computer software used in safety systems of NPP. In despite of IEEE 1012 had the latest revision in IEEE Std 1012-2012, but in the traceability analysis for the requirements can evince that IEEE Std 1012-2004 is endorsed by Regulatory Guide 1.168, Rev 2 [5]. While, in the implementation, we can refer to these versions by comparing them.

By reviewing the top tier document and develop traceability analysis, we will discover in order to use the methodology that should be completed during verification, implementation, design, validation and the requirements that should be met. By reviewing from the top tier document related to I&C system, is already the first steps in qualifying documents in other words that they have carried out requirement analysis. IEEE Std 1012-2004 not specifically discussed about I&C system for NPP, therefore to make sure which method that really matches for I&C system of NPP, in this case HTR type, we can read from additional guide from IAEA to Technical Reports Series No.384 about Verification and Validation of Software Related to Nuclear Power Plant and IAEA Specific Safety Guide No.SSG-39 [6,7].

Commonly, I&C system for nuclear is developed using Programmable Logic Controller (PLC)-based system. But since that PLC-based system had possibility for Common Cause Failure (CCF), had weakness to defense in cyber-attack, and a very expensive cost for Verification and Validation (V&V) activity, then Field Programmable Gates Array (FPGA) become an alternative because FPGA-based is a hardware so will reduce cost yet more safe because it is not a computer-based system [8,9]. To compare technology of PLC and FPGA, trade-off analysis should be developed and design criteria for the I&C system also should be reviewed to know which platform will be compatible for HTR-10 reactor. Afterwards the V&V plan must also be considered in relation to the implementation design, because this activity will take place during the development process lifecycle.
2. Theory

2.1 Instrumentation and Control System of HTR-10 Reactor

HTR-10 is a high temperature reactor–10 MW which developed by Institute of Nuclear and New Energy Technology (INET), Tsinghua University. The design of I&C system of HTR-10 had been completed since October 2000 [10]. Beforehand there are no codes and standards related to HTR-10 safety classification, but then INET had compiled the document related to machine components, I&C and electrical components[11]. HTR-10 is one of High temperature gas-cooled reactor (HTGR) type which is generation IV of nuclear energy systems and considered will have potential applications for industrial fields [1].

Commonly, I&C system of NPP were developed with software-based system to control the reactor trip function. Development of I&C system has been an important issues in NPP development since the use of computer based system for critical functions should be the first priority to handle the safety function of the NPP [12]. In the document of Standard Review Plan Appendix 7.1-A from US Nuclear Regulatory Commission (USNRC), the acceptance criteria and guidelines for I&C system and control system important to safety are discussed. In criterion 13 about I&C system, it is stated that Instrumentation shall be prepared to be able to monitor variables and systems within normal operation, for anticipated operational condition, or in accident conditions to make sure the safety, including the variables and systems which can caused of fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems [3]. In USNRC research plan, they also concern their research to I&C part, human factor and human reliability analysis, probabilistic risk assessment (PRA) and risk-informed infrastructure development [13]. HTR-10 as the advanced reactor, the design criteria shall meet the criteria from the regulatory structure from Indonesia (BAPETEN). However, since BAPETEN did not give specific standard, we could use some international guidelines.

2.2 Development of Life Cycle Model

To develop I&C system in the NPP, we have to state the process to development life cycle process for mapping the activities during the development and implementation process. For each sub-system and software, integration system should be described as management activities in development of the life cycle by choosing which model is related with the needs of our design. In document of IAEA safety standard No.SSG-39, the development of life cycle V model illustrates each step, start form requirements analysis, design specification, design implementation, and integration system. These steps should be verified and validated by the stakeholders and design criteria [14]. Figure 1 was represent development process of I&C system that should be completed to meet the criteria from stakeholders and requirement. By following this step, it will be easy to track each process to be verified.
Figure 1. I&C development life cycle processes and verification and validation activities using V model [14]

3. Methodology
3.1. Development of the trade of analysis to compare the two platforms
Development of I&C system for RDE is still considered whether will choose Programmable Logic Controller (PLC) or Field Programmable Gate Array (FPGA) as the system platform. Commonly, the reactor protection system (RPS) had been developed using PLC platform. However, since PLC need high cost for implementation, verification and validation (V&V) because of the complexity of the system, then FPGA are chosen as the alternative platform to minimize complexity, reduce common cause failure, cyber security and reduce cost of implementation [8,9]. Before setting which platform will be developed, trade off analysis between PLC and FPGA should be developed. Figure 2 represent the analytical hierarchy process to study and analyze which platform will be chosen for the I&C system of RDE, between PLC and FPGA.
3.2. Review Standards

Since BAPETEN did not state which standards should be follow and document from INET is also limited, then we can use USNRC and International Atomic Energy Agency (IAEA) documents as the guidelines to choose the codes and standards. USNRC as the global federal regulation from United Stated which is commonly used, then we can take Code of Federal Regulations (CFR) from NRC Regulation as the top tier requirement to develop traceability analysis of requirement of I&C system development. Figure 3 is represent the requirement traceability diagram that can track the guidelines to find the specific standards to develop I&C system so that the design can meet the requirement, verified and validated.

From 10 CFR document, Standard Review Plan (SRP) from USNRC and regulatory guide document which is shown in Figure 3, IEEE 1012-2004 Standard for software verification and validation was endorsed by regulatory guide 1.168 about verification, validation, reviews and audits for digital computer software used in safety systems of nuclear power plants [5]. However, since IEEE Standard for System and Software Verification and Validation has the latest version which is IEEE Std 1012-2012, therefore we can use the recent version by still paying attention what the different between 2004 and the revision in 2012.
4. Discussion

4.1 Develop V&V Plan

For the V&V activities, testing methodology will be used during implementation process. To develop testing for the system hardware and software, the methodology should follow the IEEE Std 1012-2004 or IEEE Std 1012-2012 as the latest revision. However, since we still did not state the platform that we will use whether PLC or FPGA, we should prepare and review both the standards.

Since IEC 62566 as is a specific standard related to FPGA, we can also review this standard to choose the V&V methodology. Table 1 is the task that should be followed during the development process of PLC or FPGA-based system for I&C system of NPP.

IEEE Std 1012-2004 or IEEE Std 1012-2012 as the basic requirement related to the system and software verification and validation is required to be followed even though by mixing additional methods that can be found on other standards. This will strengthen the reliability of the system.
| Process | PLC V&V Methods | FPGA V&V Methods | Recommendation |
|---------|-----------------|-----------------|----------------|
| No.1. Traceability Analysis | - Software Requirement Specification | - Software Requirement Specification | IEEE 1012-2004 |
| Failure mode and effects analysis | - interface requirements specification | - interface requirements specification | IEC 62566 |
| Analysis of defense in depth and diversity | - Hardware/software/user requirements allocation analysis[16] | - Hardware/software/user requirements allocation analysis[16] | |
| Reliability Analysis | | | |
| Validation | | | |
| Security Testing | | | |
| Analysis reliability | | | |
| Functional Requirements analysis | | | |
| 2. System Process | - System Requirement Specification | - Suitability analysis[17] | IEC 62566 |
| System Requirements | - Checks implemented in the CAD tool | - System Specification | IAEA Technical Report Series 384 |
| Hazard analysis[14] | - Functional tests on the control system platform | - Integrated system verification | |
| - On-site tests | - Validation[12] | - System Requirement | |
| - Validation | | - Formal Validation system | |
| 3. Software Process | - Software verification technique | - Code verification Static Timing Analysis[17] | IAEA Safety Standards, Specific Safety Guide No.SSG-39 |
| Functional analysis, performance analysis, security, operation, and maintenance [16]. | - Manual examination | - Formal verification[18]. | EPRI 1019181 |
| | - Static analysis | | |
| | - Dynamic Analysis | | |
| | - Elementary function of the code[12] | | |
| | - Data verification[12] | | |
| 4. Hardware Process | - Hardware requirements | - Test Bench | IEC 62566 |
| Software tool | - Hardware plan | - Test Coverage | |
| HDL-Programmed Devices Verification | - Hardware implementation | - Test Execution | |
| HPD requirement specification | - Integration test | - Static | |
| | | - Verification [17] | |
5. Conclusion

Although INET has compiled documents code and standard related to HTR-10 reactor, but since the design is still in the development stage, it seems that it is still difficult to get the reference guidelines, code and standards from Tsinghua University. But since BAPETEN did not state which code and standard should be implemented, then we can use the International guidelines and standards. Moreover, since Indonesia can do modification which is more suitable with condition in Indonesia, then requirements from the stakeholders can be considered. From the Table 1 we summarize the references from the regulatory guide, codes and standards that recommend the verification and validation methods that should be completed.

By following the guidelines from IAEA, regulatory commission, we can find rule and follow the right criteria for the development process. And it will help the licensing issues if we prepare from the beginning by develop requirement analysis. It will help approval from the regulatory body or the International regulatory commission if this design will be used for commercial by selling the design for another country.

Furthermore, for the different technology between PLC and FPGA, PLC has many tasks related to software verification, and FPGA for hardware verification. In spite of FPGA technology is based on Hardware Description Language (HPD), since FPGA still using a code to program, a software verification still needed to be developed for software application. The V&V activities is develop to ensure the correctness, accuracy, and completeness of the design by complete the concept requirement of hardware, software, and user interfaces to measure the effectiveness, the performance, foremost to meet the user needs.

Reference

[1] S.J.Ball, Holcomb D E and Cetiner S M 2012 HTGR Measurements and Instrumentation Systems
[2] Kinsey J and Hobrook M 2015 Guidance for Developing Principal Design Criteria for Advanced (Non-Light Water) Reactors
[3] US. Nuclear Regulatory Commission 2005 Standard Review Plan Appendix 7.1- A, Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety
[4] US.NRC 2007 Branch Technical Position 7-14, Guidance on Software Review for Digital Computer-Based Instrumentation and Control System Standard Review Plan
[5] US Nuclear Regulatory Commission 2013 Regulatory Guide 1.168, Rev 2, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
[6] IAEA 1999 Verification and Validation of Software Related to Nuclear Power Plant, Technical Reports Series No.384
[7] IAEA 2016 Safety Standards, Specific Safety Guide No.SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants
[8] Maerani R, Mayaka J, Akrat M El and Cheon J J 2018 V&V Plan for FPGA-based ESF-CCS Using System Engineering Approach. Journal of Physics: Conference Series vol 962
[9] Yoo J, Lee J H and Lee J S 2013 A Research on Seamless Platform Change of Reactor Protection System from PLC to FPGA Nucl. Eng. Technol. 45 477–88
[10] Xu Y 2000 The HTR-10 Project and its Further Development Inst. Nucl. energy Technol. Tsinghua Univ. Beijing, China 1. 1–8
[11] Wu Z and XI S 2002 Safety Functions and Component Classification for the HTR-10 Nucl. Eng. Des. 218 103–10
[12] IAEA 1999 Technical Report Series 384, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control
[13] US.NRC 2010 *High-Temperature Gas-Cooled Reactor (HTGR) NRC Research Plan*

[14] IAEA 2016 *IAEA Safety Standards, Specific Safety Guide No.SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants*

[15] Maerani R, Deswandri, Santoso S, Sudarno and Irianto I D 2019 Reverse Engineering Program Using MBSE to Support Development of I&C System Experimental Power Reactor from PLC to FPGA. *J. Phys. Conf. Ser.* **1198**

[16] IEEE Computer Society 2005 IEEE Standard 1012-2004 for Software Verification and Validation *Softw. Eng. Stand. Comm.*

[17] IEC 2012 *IEC 62566, Nuclear Power Plants - Instrumentation and Control Important to Safety - Development of HDL - Programmed Integrated Circuits for Systems Performing Category A functions*

[18] Flink B and Killian C 2009 *EPRI 1019181, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems*

**Acknowledgement**

This research was supported by the 2018 Research Fund of the Centre for Nuclear Reactor Technology and Safety (PTKRN -BATAN) Indonesia and Kemenristekdikti - INSINAS program 2018