V&V Methods Used in the Development of FPGA-based I&C Systems for HTR-10

R Maerani¹, TJ Suryono¹, S Santoso¹, JC Jung²

¹Centre for Nuclear Reactor Safety and Technology, National Nuclear Energy Agency of Indonesia (BATAN), Kawasan Puspiptek Serpong Gd. 80 Tangerang Selatan 15310 – Indonesia
²KEPCO International Nuclear Graduate School, Department of NPP Engineering 658-91 Haemaji-ro, Seosaengmyeon, Ulju-gun, Ulsan 45014, Republic of Korea

E-mail: maerani@batan.go.id

Abstract – Currently, in few countries, there have been many projects related to the development of Field Programmable Gate Array (FPGA)-based Instrumentation and control (I&C) system designs for their nuclear power plant (NPP), whether for modernization or the new development of NPPs. Indonesia already develops a study related to High Temperature Gas Cooled Reactor as the generation IV for NPPs type for these few years with a specific type which is High Temperature Reactor–10 MW (HTR-10). Since the FPGA-based technology is new in the field, and both the international standards and guidance, from national and international has not defined provisions this issue, therefore verification and validation (V&V) activities for this HTR-10 are mandatory to be included in the design life cycle of I&C system development to get license approval from the national regulatory body. The FPGA-based system needs concentration both in hardware and software development, but commonly only software-related standards that usually included in the design and V&V in the previous computer-based I&C system. Therefore, in this study the V&V plan needs to be developed to state the methods to be required regarding the correctness of the applications of FPGA based I&C system. By arranging this V&V method, we will see whether they are easily applicable to actual systems, had the result to reach the requirement to have reliability, availability, maintainability and safety aspects, and has shortened and easier V&V step than computer-based I&C system. From the results of this study, it can be seen that the results of the method used for V&V between Programmable Logic Controller (PLC)-based and FPGA are almost the same because both have almost the same requirements, especially in software design. Some testing is not mandatory for FPGA-based because of the reduced system complexity. The use of FPGA can shorten the V&V process which can also reduce costs.

1. Introduction

High Temperature Gas-cooled Reactor-Test Module (HTR-10) which has the first digitalize Reactor Protection System (RPS) in China, was developed by Tsinghua University of China in 2000 with their own design. The reasons for changing the analog RPS design to the digital RPS design because analog devices have many components that need a lot of space, to reduce the connection line, to avoid failure probability and the ability to online self-checking and self-diagnosis, and a friendly man-machine interface [1]. After years, microcontroller technology has disadvantages because of high complexity and rapid obsolescence. Therefore, Field Programmable Gates Array (FPGA) has become an alternative option since FPGA has a large-scale integrated circuit without an operating system, so that FPGA-based system can be more safe from cyber-attacks [2]. International Atomic Energy Agency (IAEA) also publishes the recommendation of the use of FPGA for Instrumentation and Control System (I&C...
System) for Nuclear Power Plant (NPP) in the IAEA Nuclear Energy Series document No. NP-T-3.17 [3]. Since there is no specific recommendation for FPGA development from the regulatory body, the industrial International Standards can be used for the recommendation [4].

Currently, Badan Tenaga Nuklir Nasional (BATAN) as the national nuclear agency of Indonesia, are interested to study related to High Temperature Gas Cooled Reactor (HTGR), especially to the specific HTR-10 the 10 MW reactor. Initially, the early design of HTR-10 was equipped with a digital computer-based system. However, as the increasing of the complexity of systems, the use of computer-based systems have some drawbacks, such as high development cost of modern I&C systems, software common cause failure (CCF), difficult and expensive cost of Verification and Validation (V&V) process, and regarding the obsolescence issues, it will need to retraining operational staff after installing the new software [5]. Therefore, in this study, BATAN can consider FPGA as an alternative for I&C System-based design.

Nowadays, FPGA becomes one of the alternatives to be implemented into Instrumentation and Control System (I&C) of Nuclear Power Plant (NPP). Therefore, in this study, the development of Verification and Validation (V&V) plans that are used to fulfill all the requirements of the I&C based system for the HTR-10 reactor is conducted. The V&V methods should combine the process from the requirements of the design specification of the HTGR / HTR-10 and related to the implementation of FPGA based design for I&C system.

The reasons to develop V&V plan is to ensure that the methods implemented in FPGA-based I&C system can be shorter, more accurate and can reduce costs than computer-based I&C System. The V&V methods of FPGA-based I&C System will be compared with computer-based RPS design which is developed by Tsinghua University. The V&V method still has to follow the requirement for software V&V for NPP, even though FPGA is hardware design but developed with Hardware Description Languages (HDL) and related tools used to implement the requirements in a proper assembly of the pre-developed micro-electronic resources [6]. There are similarities in requirements and processes between HDL and the software development process, syntax, or logic errors can cause the implementation errors [3]. For implementing the FPGA-based I&C system, the national regulatory body should review the design process, both hardware and software, the methodology for V&V, device failure mode information, and the result of validation related to reliability and failure analysis [3]. Therefore, this study is intended to simplify and facilitate the licensing process in the future.

2. Theory

2.1. HTR-10 I&C System

HTR-10 is a helium-cooled, pebble-bed with 10 MW power reactor, located at Tsinghua University in Beijing, China, that has similar to Siemens design for an HTR module [7]. HTR-10 took over a 10 year runtime to ensure that the system built with a high protection precision, flexible configuration, ability to self-inspection, maintainability, has stability, and reliability [8]. For the HTR-10 reactor, safety important systems are primarily the following to the RPS and its related instrumentations and power supplies, reactor shutdown systems and decay heat removal system, primary coolant pressure boundary, and its pressure relief system [9]. Figure 1 shows that the digital safety I&C system developed by Tsinghua University has many advantages, which are it is designed with a simple structure, flexible configuration, and small volume [8]. FPGA which is the latest technology than the Programmable Logic Controller (PLC) and micro-controller, comes with the promise to reduce the complexity of the developed system because the end product is a traditional analog electronics that can be designed only consisting of hardware[2].

Generally, the development of the I&C system for NPP should follow the life cycle process. The development process of the FPGA-based I&C systems has two design life cycle process: overall I&C architecture life cycle, and software development process. There are several life cycles models that can be used. However, V model is the most common life cycle process which correlates with the V&V
activities. From recommendation IAEA Safety Standards, Specific Safety Guide No. SSG-39 the development of the I&C system should follow the V&V activities that had been stated in Figure 2.

![Figure 1. HTR-10 full digital safety I&C system architecture [8].](image1)

**Figure 1.** HTR-10 full digital safety I&C system architecture [8].

2.2. **FPGA-based Instrumentation and Control System**

FPGA-based I&C system is developed with the Hardware Description Language (HDL) and related tools used to implement requirements in the micro-economics field that has been developed previously. This device is called HDL-Programmed Devices (HPD) [6]. The international standard IEC 62566, that also has a life cycle V model design as shown in Figure 3 is used to design the FPGA-based system related to the safety. Although the FPGA is hardware-based systems, and constructed using HDL language, the design must follow the software and hardware design requirements as shown in Figure 2.

![Figure 2. Life Cycle Process of I&C Development [10][11].](image2)

**Figure 2.** Life Cycle Process of I&C Development [10][11].
3. Methodology

V&V processes are used to maintain the management and development process whether for software, and hardware development to meet the requirements and user needs. The software development process should refer to the IEEE Standard 1074-2006 Standard for Developing a Software Project Life Cycle Process. And the system and software V&V process should refer to the Standard for System and Software Verification and Validation, IEEE Std 1012-2012. For the plant requirement, the design specification of HTR-10 should be made by conducting the traceability analysis from the top tier documents. All this process, including the implementation and integration should be verified. The last step is to validate the implementation design to ensure whether the design meets the requirement and work properly. The validation methods can refer to IEEE Std 1012-2012 and IEC 62566.

Although, the final product of the FPGA-based system is hardware, but since the development process uses the software tools to design and verify the application, then the validation process should be developed to check the reliability of the complex software [12].

4. Discussion

4.1. Requirement Traceability Analysis

Requirement traceability analysis is the first step verification process at the management system, to verify whether the design of the I&C system has followed the design criteria for NPP. General Design Criteria (GDC) commonly developed by the law of the nuclear regulatory commission which is a mandatory requirement for NPP development. Table 1 is the general design criteria from I&C system which is stated in GDC 13 of 10 CFR Appendix A to 50.

| Criteria                  | Requirement from General Design Criteria for NPP |
|---------------------------|--------------------------------------------------|
| 10 CFR Appendix A to 50   | Instrumentation and Control System               |
| GDC 13 for I&C System     | Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. |
Since HTR-10 is a Non-Light Water Reactor (Non-LWR), we must refer to the non-LWR design criteria. By these reasons, US. Department of Energy (DOE) with US. Nuclear Regulatory Commission (US. NRC) consider to develop a regulatory framework for non-LWR reactor which is Advanced Reactor Design Criteria (ARDC) [14]. From this report, DOE published their guidance to develop principle design criteria on December 2015 [15], and US. NRC with their Regulatory Guide (RG) 1.232 Rev.0 on April 2018[16]. This document can be used as the guidance for the reactor designers, applicants or licenses to develop non-LWR.

There is a specific design criteria related to the I&C system for the High Temperature Gas-Cooled Reactor (HTGR), by reference from RG 1.232 of US. NRC and as well as described in Figure 4, some criteria will not be different from Light Water Reactor (LWR) [11]. Table 2 compiled based on criteria from 10 CFR 50 Appendix A and guidance from RG.1.232 Rev.0.

**Table 2.** Principle Design Criteria for Non-LWR from 10 CFR 50 Appendix A, ARDC and Appendix C - Modular High-Temperature Gas-Cooled Reactor Design Criteria

| DC     | Requirement for Non-LWR                                                                 | Reg. Guide | Standards                  | Ref     |
|--------|----------------------------------------------------------------------------------------|------------|---------------------------|---------|
| MHTGR-DC-10 | Reactor design, same with GDC 10, modified for MHTGR-DC. Shall be designed with an appropriate margin. | RG 1.232. Rev.0 | IEEE Std 603-1991 | [16]     |
|         |                                                                                        | RG 1.153   |                           | [17]     |
| MHTGR-DC-13 | Instrumentation and control, shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. | RG 1.153 | IEEE Std 603-1991 | [17]     |
|         |                                                                                        |            | IEEE Std 497-1981        |         |
| MHTGR-DC-15 | Reactor coolant design, same with GDC 15, modified for MHTGR-DC 15. All systems that are part of the reactor helium pressure boundary, such as the reactor system, vessel system, and heat removal systems, and the associated auxiliary, control, and protection systems, shall be designed with sufficient margin. | RG 1.153 | IEEE Std 497-1981 | [17]     |
| GDC 19  | Control Room, shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. | RG 1.97    | IEEE Std 603-1991 | [17]     |
|         |                                                                                        |            | [18]                      |         |
| GDC 20  | The protection system shall be designed to initiate automatically the operation of appropriate systems, including the reactivity control systems. | RG 1.153  | IEEE Std 603-1991 | [17]     |
|         |                                                                                        |            | [19]                      |         |
|         |                                                                                        |            | [20]                      |         |
The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety.

The protection system independence, shall be designed to assure that the effects of natural phenomena and normal operating, maintenance, testing, and postulated accident conditions on redundant channels.

The protection system shall be designed to fail into a safe state or a state demonstrated, (Failure Modes).

The protection system shall be separated from control systems, interconnection of the protection and control systems shall be limited, shall be designed to ensure that specified acceptable system radionuclide release design limits are not exceeded during any anticipated operational occurrence, accounting for a single malfunction of the reactivity control systems.

| DC       | Requirement for Non-LWR                                                                                     | Reg. Guide | Standards                          | Ref     |
|----------|-------------------------------------------------------------------------------------------------------------|------------|------------------------------------|---------|
| GDC 21   | The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety. | RG 1.22    | IEEE Std 603-199, IEEE Std 7-4.3.2-2003 | [21]    |
|          |                                                                                                             | RG 1.171   |                                    | [22]    |
|          |                                                                                                             | RG 1.118   |                                    | [23]    |
|          |                                                                                                             | RG 1.153   | IEEE Std 379-2000 IEEE Std 338     | [17]    |
| GDC 22   | The protection system independence, shall be designed to assure that the effects of natural phenomena and normal operating, maintenance, testing, and postulated accident conditions on redundant channels. | RG 1.153   | IEEE Std 603-1991                  | [17]    |
|          |                                                                                                             | RG 1.97    | IEEE Std 497-1981                  |         |
| GDC 23   | The protection system shall be designed to fail into a safe state or a state demonstrated, (Failure Modes). | RG 1.153   | IEEE Std 603-1998 IEEE Std 379-2000 | [17]    |
| GDC 24   | The protection system shall be separated from control systems, interconnection of the protection and control systems shall be limited, shall be designed to ensure that specified acceptable system radionuclide release design limits are not exceeded during any anticipated operational occurrence, accounting for a single malfunction of the reactivity control systems. | RG 1.75    | IEEE Std 603-1991 IEEE Std 379-2000 | [17]    |
|          |                                                                                                             | RG 1.152   |                                    |         |
|          |                                                                                                             | RG 1.153   |                                    |         |

Figure 4. Design Criteria Relationship [14][24].
4.2. Verifying and Validating I&C Design Development.

Figure 5 is a computer-based I&C system for HTR-10 developed by the Institute of Nuclear and New Energy Technology (INET), Tsinghua University. They show general development from verifying design criteria, preliminary design, prototype integration, and testing before continuing to the engineering phase. Figure 6 is the design flow for FPGA-based system recommendation from NUREG/CR-7006, it shows that the development process requires hardware and software V&V.

![Diagram of HTR-10 digital I&C system development and V&V developed by INET][8]

![Diagram of FPGA Design Flow by NUREG/CR-7006][25]

From the different of software-based and hardware-based design for I&C system, the validation methods used will be different based on the characteristics of the component, programming language, complexity of the system and the environments.

Table 3 shows the V&V methods that should be complete during I&C development. Since the I&C system are related to software and hardware development, and computer-based that used in safety system of NPP and the uses of FPGA and PLC or micro controller, therefor Table 3 are referring to the international standards to develop V&V activities. Some standards are finds from the regulatory guide, and for the specific software and hardware development.
Table 3. Comparing V&V Methods between Programmable Logic Controller (PLC)/micro-controller and FPGA-based for I&C System

| No  | Verification                                      | PLC | FPGA | Validation/Testing Methods                                      | PLC  | FPGA |
|-----|--------------------------------------------------|-----|------|----------------------------------------------------------------|------|------|
| 1.  | User requirements. [26]                          | ✓   | ✓    | White-box Testing. [6] [26]                                     | ✓    | ✓    |
| 2.  | System requirements. [26]                         | ✓   | ✓    | Functional black box testing.                                   | ✓    | ✓    |
|     |                                                  |     |      | [12][26][27][28]                                                |      |      |
| 3.  | Design specification. [26]                       | ✓   | ✓    | Static Timing Analysis.                                         | ✓    | ✓    |
|     |                                                  |     |      | [6][10][25][26]                                                 |      |      |
| 4.  | Criteria analysis. [26]                          | ✓   | ✓    | Module testing. [12]                                            | ✓    | ✓    |
| 5.  | Software requirement. [26]                       | ✓   | ✓    | Reliability growth models.                                      | ✓    | ✓    |
| 6.  | System test plan. [26]                           | ✓   | ✓    | Periodic functional tests.                                      | ✓    | ✓    |
| 7.  | Software design specification. [26]              | ✓   | ✓    | Failure mode effect and criticality analysis. [10]              | ✓    | ✓    |
|     |                                                  |     |      | [12][25][26]                                                    |      |      |
| 8.  | Software Coding. [26]                            | ✓   | ✓    | Fault tree analysis. [10][25][28] (recommend for hardware system, for software should handle carefully [26]) | ✓    | ✓    |
| 9.  | System Integration. [26]                         | ✓   | ✓    | Event Tree Analysis [26]                                        | ✓    | ✓    |
| 10. | Load testing [26]                                | ✓   | ✓    |                                                                |      |      |
| 12. | Acceptance testing (formal verification) [28]    | ✓   | ✓    |                                                                |      |      |
| 13. | MC/DC (Coverage Criteria) [4][27]                | ✓   | ✓    |                                                                |      |      |

5. Conclusion

Based on the V&V process carried out on a computer-based I&C system compared to those based on FPGA, the software design process on a computer-based system has more requirements that must be met. Remembering Tsinghua University's journey as well, they took over 10 years to develop digital based I&C systems. Regarding the design flow analysis for HTR-10, the longest process was in the verifying final requirement analysis. It can be happened because the licensing process actually takes more time than process engineering, because there are so many requirements that must be met to satisfy the regulatory body. The validation testing methods for the micro-controller/PLC and the FPGA-based I&C system use the same methods, they should refer to the IEEE Std 1012-2012 for implementing the V&V process. Both micro-controller and FPGA should have a good result as the requirements from the design criteria, especially to meet the reliability, availability, maintainability and safety. To reduce the development process of FPGA-based I&C system is possible for changing the obsolete components, or for the safety reasons to avoid cyber-attacks that must be replaced from computer–based system to hardware–based system. By replacing the old one, the design requirements verification process has been carried out, so that the reverse engineering can be carried out based on the previous operational records, and develop the software requirement specification for FPGA-based system, develop design synthesis for FPGA-based system, implementation and integration. This study explains that although FPGA is a different platform from PLC and other software based, since it related to components that are important for safety, they have the same mandatory of requirements.
Acknowledgments
This research is funded by DIPA of the Centre for Nuclear Reactor Technology and Safety (PTKRN - BATAN) and INSINAS Ristek-BRIN the Ministry of Research and Technology of 2021 fiscal year.

References
[1] Li F, Yang Z, An Z and Zhang L 2002 The First Digital Reactor Protection System in China Nucl. Eng. Des. 218 215–25
[2] Mayaka J and Jung J C 2018 Complexity reduction of the Engineered Safety Features Component Control System Nucl. Eng. Des. 331 194–203
[3] IAEA 2016 IAEA Nuclear Energy Series No. NP-T.3.17, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants
[4] Maerani R, Mayaka J K and Jung J C 2018 Software Verification Process and Methodology for the Development of FPGA-based Engineered Safety Features System Nucl. Eng. Des. 330 325–31
[5] IAEA 1999 Technical reports series No. 387, Modern instrumentation and control for nuclear power plants: A Guidebook vol 1
[6] 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
[7] Medowell B, Mitchell M, Pugh R, Nickolaus J and Swearingen G 2011 High Temperature Gas Reactors : Assessment of Applicable Codes and Standards
[8] Wei L, Liu L and Yang Z 2011 Design, application and maintenance of HTR-10 full digital safety I&C system Proc. 2011 Int. Conf. Mechatron. Sci. Electr. Eng. Comput. MEC 2011 450–3
[9] International Atomic Energy Agency 1998 Safety related design and economic aspects of HTGRs
[10] IAEA 2016 IAEA Safety Standards, Specific Safety Guide No.SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants
[11] Maerani R, Suryono T J and Subekti M 2019 Requirement Analysis of Computer-Based Instrumentation and Control System for Reaktor Daya Eksperimental J. Teknol. Reakt. Nukl. Tri Dasa Mega 21 39
[12] Flink B and Killian C 2009 EPRI TR-1019181, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems
[13] Anon NRC: 10 CFR Appendix A to Part 50—General Design Criteria for Nuclear Power Plants
[14] Holbrook M R 2015 Summary of The Advance Reactor Design Criteria (ARDC) Phase 1 Activities, Including the Development of Final Report and the Advanced Reactor Technology
[15] Kinsey J and Hobrook M 2015 Guidance for Developing Principal Design Criteria for Advanced (Non-Light Water ) Reactors
[16] US.NRC 2018 Guidance for Developing Principal Design Criteria for Non-Light Water Reactor, Regulatory Guide 1.232, Rev 0
[17] US.NRC 1996 Regulatory guide 1.153 - Criteria for Safety Systems
[18] US.NRC 1980 Regulatory Guide 1.97, Instrumentation for Light Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following and Accident
[19] US.NRC 2003 Regulatory Guide 1.196, Control Room Habitability at Light-Water Nuclear Power Reactors
[20] US.NRC 2003 Regulatory Guide 1.197, Demostrating Control Room Envelope Integrity at Nuclear Power Reactors
[21] US.NRC 1972 Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions
[22] US.NRC 2013 Software Unit Testing for Digital Computer Software used in Safety System of Nuclear Power Plants Regulatory Guide 1.171 vol 17 pp 1–14
[23] US.NRC 1978 Regulatory Guide 1.118, Periodic Testing of Electric Power and Protection Systems
[24] Holbrook M R 2015 Summary of the Advanced Reactor Design Criteria ( ARDC ) Phase 2
Activities

[25] Bobrek M, Bouldin D, D.E H, S.M K, S.F S, C W and Wood R T 2009 NUREG/CR-7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems
[26] IAEA 1999 IAEA Technical Report Series No.384, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control
[27] Ahmed I, Jung J and Heo G 2017 Design Verification Enhancement of Field Programmable Gate Array-Based Safety-Critical I&C System of Nuclear Power Plant Nucl. Eng. Des. 317 232–41
[28] IEEE 2012 Standard for System and Software Verification and Validation, IEEE Std 1012-2012