Reverse Engineering Program Using MBSE to Support Development of I&C System Experimental Power Reactor from PLC to FPGA.

Restu Maerani*, Deswandri, Sigit Santoso, Sudarno, Ign. Djoko Irianto
Centre for Nuclear Reactor Safety and Technology, National Nuclear Energy Agency of Indonesia (BATAN), Kawasan Puspiptek Serpong Gd. 80 Tangerang Selatan 15310, Indonesia

*E-mail: maerani@batan.go.id

Abstract. Indonesian Experimental Power Reactor (RDE) basic design is designed by refer to the High Temperature Gas-cooled reactor-test Module (HTR-10) type which developed by Tsinghua University in China since 1995 and receiving the first critically on December 2000. Currently, the market for a control system in nuclear power plant (NPP) industry is using micro-controller and Programmable Logic Controller (PLC). Since the computer-based technologies are vulnerable to cyber-attack possibility, software common cause failure (CCF) and system complexity, however, development of RDE designs should be thought of by the latest technologies in accordance with the development of Instrumentation and Control (I&C) system which play an important role in maintaining the safety aspect for NPP. This study deals with the reverse engineering program for I&C with the PLC-based system, to obtain the design specification from the previous design in order to improve its reliability by considering systems hardware using Field-programmable Gate Array (FPGA) as an alternative platform. Before developing reverse engineering should analyze why FPGA become an alternative system to change the PLC-based system. Reverse engineering process will cover by model-based system engineering (MBSE), which is the formal modeling application to support systems requirements, design, analysis, verification and validation (V&V) activities. The process starting with the conceptual design, requirement analysis, continuing throughout development and later life cycle phases which is recommended using V model. It is hoped that by doing this reverse engineering program, there is an analysis function related I&C system so that the more reliable design with the use of FPGA-based platform can be made. Reverse engineering can also help to track back the original development with I&C platform from the licensing requirement so that to develop re-engineering program for the new FPGA-based I&C system can meet the design criteria and accepted by the regulatory commission. The requirement, selection of lifecycle model, and verification methodology will be will be explained clearly in order to become a reference in the development plan of RDE in Indonesia.

Keywords: MBSE, reverse engineering, re-engineering, HTR-10, PLC, FPGA
1. Introduction

Indonesia had developed the basic design of Experimental Power Reactor (RDE) by National Nuclear Energy Agency of Indonesia (BATAN). RDE basic design is developed by refers to design of High Temperature Gas-cooled reactor-test Module (HTR-10) type which developed in China from Tsinghua University since 1995 and reaches its critically on December 2000 [1]. RDE with an HTR-10 type is by applying pebble bed reactor technology which is chosen with the consideration that a High Temperature Gas Reactor (HTGR) type is a very safe, fuel flexibility, a competitive price, multipurpose and can be developed in any region in Indonesia as needed. Technology digital of Instrumentation and Control (I&C) system with Programmable Logic Controller (PLC) platform already implemented and licensed in several types of reactor since 1980 [2,3] Digital I&C system is developed to simplify the operations and maintenance staff to better anticipate, understand, and respond to any potential conditions in plant [4,5]. I&C system as the safety critical system which plays an important role to shut down the reactor and to actuating the Engineered Safety Features while in accident condition, to prevent damage to the plant and release of radioactive material. By this reasons, the system performance of I&C system shall be developed with a high level of reliability, and availability thus leading to a higher safety [4,5]. According to Burzynski state in 2017[6], there is 40 percent which is 450 nuclear reactors have improvement technology for the I&C system. And for the recent of 60 reactors which still under construction will develop methods to modify previous technologies for the digital I&C system.

Currently, Field Programmable Gate Array (FPGA) is the new Integrated Circuit (IC) digital that is reliable and has the recommendation from Nuclear Regulatory Commission (NRC) and International Atomic Energy Agency (IAEA) to be implemented in the NPP I&C system[3]. FPGA platform can be applied to perform functions which is related to safety-critical and require high reliability, like RPS in I&C system of Nuclear Power Plant (NPP), automobiles or aircraft control [7].

Based on the IAEA recommendations that all I&C activities associated with the development, implementation, and operation of the overall I&C architecture, individual I&C systems, and I&C components should be carried out in the framework of a documented development life cycle [8,9]. Since we will implement FPGA technology, we should look for regulatory standard reference document related to the use of FPGA for NPP. However, FPGA specific standards are not found in the United States Nuclear Regulatory Commission (USNRC) so that we can use alternative documents from the International Electrotechnical Commission IEC 62566: 2012 and EPRI Technical Report 1019181 as the guidelines [3,8]. In IEC 62566:2012 and EPRI TR 1019181 is recommend to use V model life cycle for development of HDL-Programmed Devices (HPD), therefore the selected life cycle model was a selection of model-based system engineering that will assist the reverse engineering process for I&C system RDE as the system engineering activity [10,11].
Based on information in Figure 1, the V model development life cycle activities are related to constituting engineering:

- Requirements analysis, identifying requirements for all external and internal interactions and interfaces
- Functional analysis and design (functional definition): focusing on modular configuration.
- Component design (physical definition): designing and prototyping all components,
- Design validation: testing and evaluating system component.

The purpose of this study is to review the upstream documents which refer to design criteria of the I&C system, component, hardware and software related to safety and non-safety in developing the previous design of I&C system, especially an HTR-10 type if possible. In developing and the use of FPGA for NPP should decompose the design specification and follow the requirement specification from the previous design which is the PLC-based I&C system. And also to prepare the studies technology assessment related to FPGA to be developed in I&C system, by the guidelines of MBSE how the use of life cycle model for reverse engineering, or development of I&C system with FPGA platform understanding their impact on system performance, and to choose the testing methods for the verification process.

2. Theory

2.1 Instrumentation and Control of HTR-10

HTR-10 I&C system had developed with fully digital safety system as well as the other reactor type. There are three major activities should be concerned with developing HTGR digital I&C system; advanced instrumentation, advanced controls, advanced diagnostics and prognostics[12]. The performance requirements for an HTGR’s instrumentation system came from the functional requirements, which describes the physical characteristics of the components and potential accident scenario [13], it also discussed in the guidance to develop general design criteria for advanced reactor (non-light water) reactor [14]. Therefore, in the phase of requirement analysis, functional requirements of RDE I&C system should follow the requirements standard document in order to achieve high performance of the system.
2.2. Model-Based System Engineering for Reverse Engineering

2.2.1 Model-Based System Engineering (MBSE)
MBSE is a formal modeling to represent systems requirements, conceptual design, architecture, design implementation, V&V activity and continuing the life cycle phases. There is many models of design life cycle was created and applied in the development process of system or software [15]. MBSE can help the system engineer to maintain the seven major in the development process; state the problem, investigate alternatives, model the system, integrate each function, launch the system, assess performance, and re-evaluate by developing validation activity [16]. The v model design life cycle is recommended for the development of an FPGA-based I&C system for RDE by the guidelines of IEC 62566 and EPRI Technical Report 1019181 [10,11].

2.2.2 Reverse Engineering
Reverse Engineering is developing to analyzing a system in order to identify the components of the system as well as to create representations of the system to a higher level [17]. The reason to develop reverse engineering program is to improve the design of I&C system for RDE using FPGA platform is to reduce the complexity of the system, avoid CCF, security aspect and for the reliability and availability system. In some cases, time performance of the system also caused to develop reverse engineering [3]. After developing reverse engineering program, we can develop re-engineering by reconstructing RDE I&C system with FPGA platform. Figure 2 is an example of a reverse engineering life cycle model which is the opposite of forwarding engineering V model, where the implementation of the activity starts by looking back validation criteria. Before starts the reverse engineering program we should think about design features or measures that support maintenance, modification or replacement in the future [6].

![Figure 2. Reverse Engineering Life Cycle [15,17.]](image)

3. Methodology
Methodology for reverse engineering program in the development of I&C system for RDE should follow the requirement in IEC 62566 or EPRI TR 1019181 which is to use V life cycle model as described in Figure 1. But as the system engineering methods, MBSE will guide the requirement analysis, development and V&V activity by system engineering approach. In the discussion, each section will represent each step should be done in preparing reverse engineering program and re-engineering program in the development of I&C system for RDE.
4. Discussion

4.1. Conceptual Design

4.1.1 Conceptual Design Instrumentation and Control System for HTGR
The design is the process to define and select the solution to meet the criteria of requirements both for process and product [18]. The base of HTGR type I&C system design is similar to the other type of reactor, which have the same safety criteria with the industry safety standards that had been applied to the previous type of reactor. The conceptual design for I&C system is transfer directly from Light Water Reactor (LWR) to HTGR, both for safety-related and non safety-related system. The performance requirements for an HTGR’s instrumentation system is coming up from the functional requirements, which have to concern with the physical characteristics and potential accident scenarios [19]. By following the regulatory guide and recent technology from the nuclear industry, we have to achieve safe system, reliable and measures the effectiveness by the cost. By this reason, we have to improve and concern to minimize the impact of obsolescence, avoid CCF and cyber attack, reduce operating and maintenance costs [6].

The architecture design of the overall I&C system is based on the defense-in-depth and diversity concept [20]. The conceptual design was carried out in two stages, concept exploration and concept definition;

- Concept Exploration
The purpose of this phase is to explore ideas and technologies and examine potential concepts. The proposed system would meet the regulatory requirements criteria, utility requirements, and industrial codes and standards. The output of this phase is the system performance requirements related to I&C system using FPGA platform.

- Concept Definition
Definition of the functional architecture, as well as the functional flow diagram, should be designed at this stage. By examines, alternative concepts which are FPGA based system, define functional and physical architectures of an I&C system for RDE, selects the preferred concept on the basis of performance, cost, schedule, and risk, and defines system functional specifications for the I&C system of RDE with an HTR-10 type.

The conceptual design which shown in Figure 3, should follow the guidelines from the regulatory standards about the functional requirement for the I&C system before it represented in design architecture and design synthesis. The FPGA-based I&C system can be considered as an alternative platform besides PLC, from price or needs consideration, safety, availability, reliability, etc.
4.2 Trade-Off Analysis

Trade-off analysis is used to balance performance, risk, cost, and schedule for physical design. In this reverse engineering program, trade-off analysis is developed to compare the performance of PLC platform and FPGA platform. Figure 4 represents the analytical hierarchy process to check the performance of the system. This studies can be developed by collecting data from the previous platform which is PLC, then compare with FPGAs performance.

4.3 Requirement Analysis

4.3.1 Licensing Requirements

The process of digital I&C certification in the nuclear industry starts when the utility presents an I&C design and its associated quality evidence to the regulator; the regulator will then determine whether the presented I&C system meets the mandatory safety requirements prescribed in regulations [8,22]. Figure 5 shows the regulatory structure for NPP development in Indonesia that the top tier document should start from the requirement of constitution 1945, and BAPETEN as the regulatory body in Indonesia also guide with the state from the chairman of BAPETEN related to NPP development by guidelines from IAEA.
4.3.2 Performance Requirements Analysis

The performance requirements for an HTGR's instrumentation system came from its functional requirements, which in turn derive from the plant's physical characteristics and potential accident scenarios. The instrumentation system's basic safety function can be expressed in how it supports the plant's three fundamental safety functions [19]:

- Confinement of radioactive material,
- Control of the core reactivity,
- Removal of the heat from the core.

4.3.3 Functional Requirements Analysis

The functional requirements for the I&C system should be reviewed referring to the Title 10 of the Code Federal Regulation (10 CFR) Part 50, as described in Standards Review Plan (SRP) Chapter 7.1 and the individual SRP section [23]. The functional requirements for any component of the I&C system are strongly dependent upon the role of the component in the system architecture [24].

For the I&C system of NPP, the development process is divided into two processes which is system design and software or digital computer design. For the system component related to safety I&C system, based on IEEE Std 603-2009 requires that [25]:

- Sense and command features;
  - Automatic control
  - Manual control
  - The interaction between the sense and command features and another system
  - Derivation of system inputs
  - Capability for testing and calibration
Operating bypasses
- Maintenance Bypasses
- Setpoints
- Execute Features
  - Automatic control
  - Manual control
  - Completion of protective action
- Operating bypasses

**Figure 6. Requirement Traceability Related to I&C System of NPP**

For digital computer-based systems, the evaluation should confirm that the general functional requirements have been appropriately allocated into hardware and software requirement [26]. For the development of software or digital computer for I&C system, based on Branch Technical Position (BTP) 7-14 reviews, the functional requirements should describe [27]:

- How each function is initiated
- The input and output variables required of the function
- The task sequences, actions, and events required to carry out the function
- The termination conditions and system status at the conclusion of the function.

Figure 6 above represented the top tier requirement from the general design criteria for development of I&C system, which had been stated in 10 CFR and guidelines from the regulatory guide how to use and select the International standards. Since the requirement in Figure 6 is still for general design criteria of I&C system, for the implementation of FPGA-based I&C system RDE should refer to this requirement and can decompose the system by the needs and characteristics of the HTR-10 type.

**4.3.4 Requirements Verification Traceability Matrix**
Table 1. RVTM Relation between IAEA Safety Standards and International Standards [9]

| Design Specification | Design Requirements | Guidelines | Standards | Requirement Type |
|----------------------|---------------------|------------|-----------|-----------------|
| Provision of Instrumentation | Instrumentation shall be provided for: determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems, and the containment at the NPP. | SSR-2/1 (Rev.1) Requirement No. 59 | SSR-2/1 (Rev.1) Requirement No. 60 | Shall |
| Control System | Appropriate and reliable control systems shall be provided at the NPP to maintain and limit the relevant process variables within the specified operational ranges. | IEEE 603 | Shall |
| Protection system | A protection system shall be provided at the NPP that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions. | SSR-2/1 (Rev.1) Requirement No. 61 | Shall |
| Reliability and testability of instrumentation and control systems | I&C systems for items important to safety at the NPP shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed. | IEC 60671, IEC 338 | Shall |
| Computer-based equipment in systems important to safety | Development and testing of computer hardware and software shall be established and implemented throughout the service life of the system. | IEC 62566, IEEE 1012, IEEE Std. 1074 | Shall |
| Separation of protection systems and control systems | Interference between protection systems and control systems at the NPP shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence. | SSR-2/1 (Rev.1) Requirement No. 64 | Shall |
| Control room | A control room shall be provided at the NPP from which the plant can be safely operated in all operational states, either automatically or manually | SSR-2/1 (Rev.1) Requirement No. 65 | Shall |
| I&C | All structures, systems, and components, including software for I&C, that are items important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety | Requirement Safety Guide No. NS-G-1.9 | Shall |

IAEA Specific Safety Requirements No.SSR-2/1 (Rev.1) has requirements shall be met to develop the structures, systems, and components of a nuclear power plant, as well as for procedures and organizational processes important to safety [28]. And for the specific design for I&C system development, the IAEA Safety Standards, Specific Safety Guide No.SSG-39 has guidelines for the design and implementation, system integration until system validation that can be followed [29].
By referring this statute, we can analyze the performance requirements and functional for the I&C system. Table 1 shows the relation between IAEA safety standards requirement with the International standards related to each system and component for the I&C system which has a specific requirement for example; IEC 62566 for the use of hardware description language, in this case, FPGA.

4.4 FPGA-based System Design and Implementation

For the design and implementation of FPGA based system, the development process should refer to IEC 62566 which have guidelines for an HDL-Programmed Devices (HPD). By this IEC 62566 standards, it requires activities that must be fulfilled [10]:

- The development process shall define a design phase and an implementation phase.
- Even though the use of specific languages and tools cannot be required, the following may be considered as common basic rules for languages and tools used for the design and implementation of HPDs for class 1 systems.
- The use of the language should be restricted to a “safe” subset where appropriate, for example, be restricted to features that are needed to implement the required functions and are synthesis-able with standardized libraries (e.g. avoid the use of initial values, explicit delays or division).
- Starting from the HPD requirement specification, the design initially aims at defining major choices such as the decomposition into modules.

5 Verification and Validation

In the process of verification and validation (V&V) of the design, verification plan should be developed to choose which standards and methods will be followed to verify the system and software in I&C development. Since the implementation will develop the FPGA-based system, the standard for system and software should follow IEC 62566 [10], IEEE 1012-2012 [30] and for additional guidelines can follow IAEA Technical Report Series No. 384 [31].

Before developing software design implementation, verification and validation stage, in the early development should state the software requirement specification SRS. The guideline of RSR can be found in regulatory guide 1.172 [32]. Since the development of the FPGA-based system is using VHDL code to give comment action to the I&C components, the standards document to be followed should add the requirement for VHDL code, which is; IEEE 1076-2008, or the guideline from NUREG/CR-7006 [33,34].

For the verification methodology, usually, software testing is developed to check the input/output of the VHDL code. For the VHDL verification testing methods is shown in Figure 7. For the software verification methodology can be developed [35]:

- White-box testing
- Modified condition/decision coverage (coverage test)
- Software reliability testing using a growth model
- Static timing analysis
6 Conclusion

Development of I&C system for RDE must follow the recent technology for a digital I&C system of the nuclear power plant. For the safety aspect, the simplicity of the system become the big option considering that I&C system has complexity issues regarding integrated control system of the plant. By this reasons, it is necessary to develop an I&C system with new technology which is the FPGA-based I&C system. For the requirement analysis phase, the functional analysis of each component of HTR-10 is similar to another type of reactor. The most important is to develop requirement traceability to map back the regulatory structure of the originally I&C system based on PLC platform related to functional requirements to be synthesized into the new FPGA-based system. For the detailed architecture of FPGA based I&C system for RDE is needed to develop in the future.

It is necessary to use model-based system engineering to manage reverse engineering, reengineering process for development of I&C system which is related to the safety of NPP that requires detail process. By referring system engineering process which represents in design lifecycle-MBSE, its hopes that development of detail design RDE will be verified, validate and accepted to the nuclear regulatory commission.

Acknowledgment
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.

References

[1] Chen F, Dong Y and Zhang Z 2016 Post-test Simulation of the HTR-10 Reactivity Insertion Without Scram Ann. Nucl. Energy 92 36–45

[2] Maerani R and Jung J C Improve ESF CCS based FPGA Design Life Cycle Using Y Model for Development Proses 2017 Systems Engineering Model Based System Engineering - Korea System Engineering Society Spring Conference 2017

[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] Mayaka J and Jung J C 2017 Complexity Analysis of an FPGA-Based ESF-CCS ISOFIC 2017, Gyeongju, Korea, November 26-30, 2017 pp 1–8

[5] Rudolf B 2017 Modernization of NPP â€™s Safety I & C - Challenges and Solutions ISOFIC 2017, Gyeongju, Korea, November 26-30, 2017 pp 1–5

[6] Burzynski M J 2017 Case For The Adoption Of FPGA Technology In The Implementation And Replacement Of Equipment And Systems In Nuclear Power Plants ISOFIC 2017, Gyeongju, Korea, November 26-30, 2017 pp 1–10

[7] Farias M S, Martins R H S, Teixeira P I N and Carvalho P V R 2016 FPGA-Based I&C systems in Nuclear Plants Chem. Eng. Trans. 53 283–8

[8] Maerani R, Mayaka J, Akrat M El and Jung J C 2018 V & V Plan for FPGA-based ESF-CCS Using System Engineering Approach . International Conference on Nuclear Technologies and Sciences (ICoNETS 2017), Restu Maerani et al 2018 J. Phys.: Conf. Ser. 962 012007

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

[10] 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, IEC 62566, The International Electrotechnical Commi

[11] Fink R, Killian C and Nguyen T 2011 Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems

[12] Jr T I W, Poore W P, Harrisin T J and Joseph R . 2010 Task 1- Control and Protection System in VHTRS For Process Heat Application, Oak Ridge National Laboratory

[13] Holcomb D E 2012 HTGR Measurements and Instrumentation Systems

[14] Kinsey J and Hobrook M 2015 Guidance for Developing Principal Design Criteria for Advanced ( Non-Light Water ) Reactors

[15] Estefan J A 2008 Survey of Model-Based Systems Engineering ( MBSE ) Methodologies INCOSE MBSE Initiat.

[16] Karban R, Andolfato L, Bristow P, Chiozzi G, Esselborn M, Schilling M, Schmid C, Sommer H and Zamparelli M 2014 Model Based Systems Engineering for Sthrownical Projects Modeling, Systems Engineering, and Project Management for Astronomy VI vol 9150

[17] Hasan M M, Elakrat M, Mayaka J and Jung J C 2017 Application of Sequence Diagram to The Reverse Engineering Process of The ESF-CCS Model Based System
Engineering - Korea System Engineering Society Spring Conference 2017

[18] Lee J S and Miller L E 2007 INCOSE - Systems Engineering Handbook

[19] Holcomb D E, Ball S J and Cetiner S M 2012 HTGR Measurements and Instrumentation Systems I

[20] Wei-Jun Tian Ya-Jie Dong Xiao-Sheng Zhang li ming Liu Guang-Ming Jiang Guo-Jin H Reactor Protection Diversity Requirements and the Typical Solution Base on DCS Proceedings of the 18th International Conference on Nuclear Engineering ICONE18 May 17-21, 2010, Xi’an, China

[21] Kossiakoff A, Sweet W N, Seymour S J and Biemer S M 2011 Systems engineering principles for the design of biomedical signal processing systems vol 2

[22] Yih S and Fan C-F 2012 Analyzing the decision making process of certifying digital control systems of nuclear power plants Nucl. Eng. Des. 242 379–88

[23] US.NRC 1997 NUREG-0800, Branch Technical Position HICB-14. Rev-4, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

[24] Brill R W and Johnson G 2000 A Structured Approach for the Review of Digital System Requirements Specifications for Nuclear Power Plant International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies

[25] IEEE 2009 Standard Criteria for Safety System for Nuclear Power Generating Stations

[26] US. Nuclear Regulatory Commission 1997 NUREG-75/087, Appendix 7.1.C Guidance for Evaluation of Conformance to IEEE Std 603 Standard Review Plan

[27] US. Nuclear Regulatory Commission 2007 NUREG-0800, BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control System”

[28] IAEA 2000 IAEA Safety Standards, Specific Safety Requirements No.SSR-2/1 (Rev.1), Safety of Nuclear Power Plants: Design vol 1

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

[30] IEEE 2012 Standard for System and Software Verification and Validation, IEEE Std 1012-2012, IEEE Computer Society, New York, USA

[31] IAEA 1999 Technical Report Series 384, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control

[32] US. NRC 2013 Software Requirement Specification for Digital Computer Software and Complex Electronics Used in Safety System of Nuclear Power Plants Regulatory Guide 1.172

[33] Maerani R and Jung J C 2017 VHDL Verification of FPGA based ESF-CCS for Nuclear Power Plant I & C System ISOFIC 2017, Gyeongju, Korea, November 26-30, 2017 pp 1–6

[34] Bobrek M, Bouldin D, Holcomb D E, Killough S M, Smith S F, Ward C and Wood R T 2009 Review Guidelines for Field-Programmable Gate Array in Nuclear Power Plant Safety System - NUREG/CR-7006

[35] 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