Tri Dasa Mega Vol. 21 No. 1 (2019) 39–46

Jurnal Teknologi Reaktor Nuklir

Tri Dasa Mega

Journal homepage: jurnal.batan.go.id/index.php/tridam

Requirement Analysis of Computer-Based Instrumentation and Control System for *Reaktor Daya Eksperimental*

Restu Maerani*, Tulis Jojok Suryono, Muhammad Subekti

Center for Nuclear Reactor Technology and Safety, National Nuclear Energy Agency of Indonesia (BATAN), Kawasan Puspiptek Serpong Gd. 80 Tangerang Selatan 15310, Indonesia

ARTICLE INFO

Article history:

Received: 28 January 2019
Received in revised form: 1 March 2019
Accepted: 1 March 2019

Keywords:

Computer-based system
I&C System
Requirements analysis
Licensing
RDE

A B S T R A C T

Developing and licensing of digital Instrumentation and control (I&C) system for nuclear power plant (NPP) are challenging especially for the new construction since digital technology are composite with a very high complexity of many integrated systems. National Nuclear Energy Agency of Indonesia (BATAN), who design *Reaktor Daya Eksperimental* (RDE), should prepare the documents to meet the licensing requirements of national regulator in this case Nuclear Energy Regulatory Agency of Indonesia (BAPETEN). BAPETEN's chairman regulation No.6 year of 2012 is the first national requirement which state requirements related to design of computer-based system concerning on safety of power reactor that should be followed. Since BAPETEN only denotes requirements without state which code and standards to be used, therefore BATAN can add references from International Nuclear Energy Agency (IAEA) guidelines. In this paper, requirement document traceability is developed to determine which code and standards should be used to verify and validate the I&C computer-based system of RDE. The hierarchy of regulatory and utility requirements are developed to guide the design basis documentation. Developing requirements analysis of computer-based I&C system RDE are completed after determining the design requirements from the utility and regulatory requirements. This methodology will help the design engineers to follow the utility requirements by concerning to the production, and follow the regulatory requirements concerning the safety aspect.

1. INTRODUCTION

National Nuclear Energy Agency of Indonesia (BATAN) has a plan to develop the Experimental Power Reactor which is a High Temperature Gas-Cooled Reactor (HTGR) type. This project will be the first experience for Indonesia to construct nuclear power plant (NPP). Therefore, currently BATAN is preparing a required document for licensing issues by completing requirement analysis process that should be submited to Nuclear Energy Regulatory Agency of Indonesia (BAPETEN).

The design of Reaktor Daya Eksperimental (RDE) refers to the design of High Temperature Reactor (HTR)-module and 10 MW High Temperature Gas-cooled Test Reactor (HTR-10). Firstly, a HTR-10 was developed by Institute of Nuclear and New Energy Technology (INET) of Tshinghua University, China which reached its critically in 2003 [1]. Considering that this project is the first time for Indonesia, there are some documents that should be prepared regarding licensing requirements of RDE developed by BATAN. With the challenge of designing

*Corresponding author. Tel./Fax.: +62-21-7560912
E-mail: maerani@batan.go.id
DOI: 10.17146/tdm.2019.21.1.5312

instrumentation and control (I&C) system which currently use computer-based system as the digital technology replacing analog equipments, the design engineers colaborated with the system engineers should concern to the complexity of the I&C system since it is related to safety functions [2].

I&C systems in NPP play an important role since they are being used in control system, reactor protection systems and acquisition of sensor measurement data from the major components [3]. From the general design principle, it is also explained that the I&C system is developed to have relation with the design and implementation process to confirm that requirement analysis for the process of the system components and equipments is verified [4].

I&C system should be developed by considering common cause failure (CCF), cost effectiveness, reducing system complexity, and the cyber security aspects since I&C system is a major component to control and protecting the NPP [5].

Process for licensing issue takes the longer part than the development phase because usually national regulations are difficult to understand because of the lack of information and only show the general appearance, therefore coordination with international are needed to find the solution.The requirement analysis process should be able to describe the user needs, technical and physical requirements based on design criteria of RDE as the advanced non Light Water Reactor (non- LWR) [2, 6].

In this paper, authors try to gather international guidelines from International Atomic Energy Agency (IAEA), United State Nuclear Regulatory Commission (USNRC), codes and international standards which traceable from the international guidelines which is still sugest the same requirements. The reasons why USNRC guidelines used for this analysis are US regulator has completed example and commonly-used in many countries.

Since General Design Criteria (GDC) for non-LWR reactor with specific to HTGR is not available, thus in this paper the authors adopt from the 10 of the Code of Federal Regulations (10 CFR) Part 50 Appendix A for Light Water Reactor type (LWR) with a guideline from Regulatory Guide 1.232 [7]. GDC determines structures, systems, and components (CCSs) important to safety which are needed to meet the performance requirements. The GDC issue should be completed in future study related to HTGR.

It is important to develop this research, because it requires agreement between RDE designers to follow the same reference documents to meet the requirements from BAPETEN. Beforehand, BATAN should specify the national and international regulation as the design basis document. This method will simplify the designers to develop the requirements traceability analysis to discover the recommended codes and standards. The purpose of these requirements analysis will help BATAN to get the license of developing the computer-based I&C system.

2. THEORY

2.1 HTR-10 Reactor

The first gas-cooled reactor was proposed in 1942 at the University of Wisconsin, United States [8], and developed in Germany in the last of 1950 [9]. The name HTR-10 refers to the prototype of high temperature gas-cooled reactor developed by INET with the capacity of 10 MW [8]. The design of I&C system of HTGR is designed with inherent and passive safety features for accident condition to allow that the type of the reactor will have a little potential damage. HTR-10 as reference design for RDE is equipped with the control rod function, hence it can cause the reactor to automatically shutdown [10].

HTR-10 has three-vessel type design which is similar with Gas Turbine-Modular Helium Reactor (GT-MHR) [8]. **Table 1** shows the plant description of the HTR-10.

Table 1. HTR-10 Plant Description[8]

No	Key Specification	
1	Thermal Power	10 MW
2	Power Density	2 MW/M^3
3	Secondary Coolant	Steam
4	Primary System Pressure	3 MPa
5	Primary Inlet Temperature	250 ^{o}C
6	Primary Outlet Temperature	700 ^{o}C
7	Vessel Material	C-Mn-Si Steel
8	Core Type	Pebble Bed
9	Year of Operation	Start Up in 2000

2.2 Principle Design Criteria for Non-Light Water Reactor

Regulatory guide is developed to organize and guide an acceptable methodology that should be followed to meet the requirements from the regulatory commission [11]. RG 1.232 of USNRC states that GDC from 10 CFR Part 50 Appendix A can be adopted for Non-LWR. This RG is about a guidance for developing the Principal Design Criteria (PDC) for Non-LWR which is specific for sodium-cooled fast reactors (SFRs), and modular high temperature gas-cooled reactors (MHTGRs) [7]. RG 1.232 also states that the design of non-LWR will use more simply the passive design by

decomposed the new design features related to the safety and security functions, modified from GDC Appendix A [7]. By this reason, GDC for specific HTGR is a challenge to be completed in order to help designers of HTR-10 to meet the criteria of regulatory requirement.

GDC is important to be created because it identifies the design requirements from the regulator, and there are many requirements that should be analyzed during the development process. **Table 2** illustrates the responsibility of the analyst and designer to complete the requirement tasks for their responsibility.

Table 2. Layer of Requirements and Role[12]

Layer of Requirements	Domain	View	Role
Stakeholder's Requirements	Problem	Stakeholder	State what the stakeholders want to achieve through the system.
System Requirements Analysis	Solution	System Analyst	State abstractly what the system will do to meet the stakeholder requirements
Architecture Design	Solution	Designer	State how the specific design will meet the system requirements

2.3 Instrumentation and Control System for HTR-10

Currently there are no specific criteria related to I&C for HTR-10. However since this system will be operated in a high temperature environment, there is important attention need to be concerned; and there are information need to collect for developing criteria to measure the qualification of hardware and software related to I&C system [13].

Fig. 1 represents the need of a high temperature materials which producing the final steam.

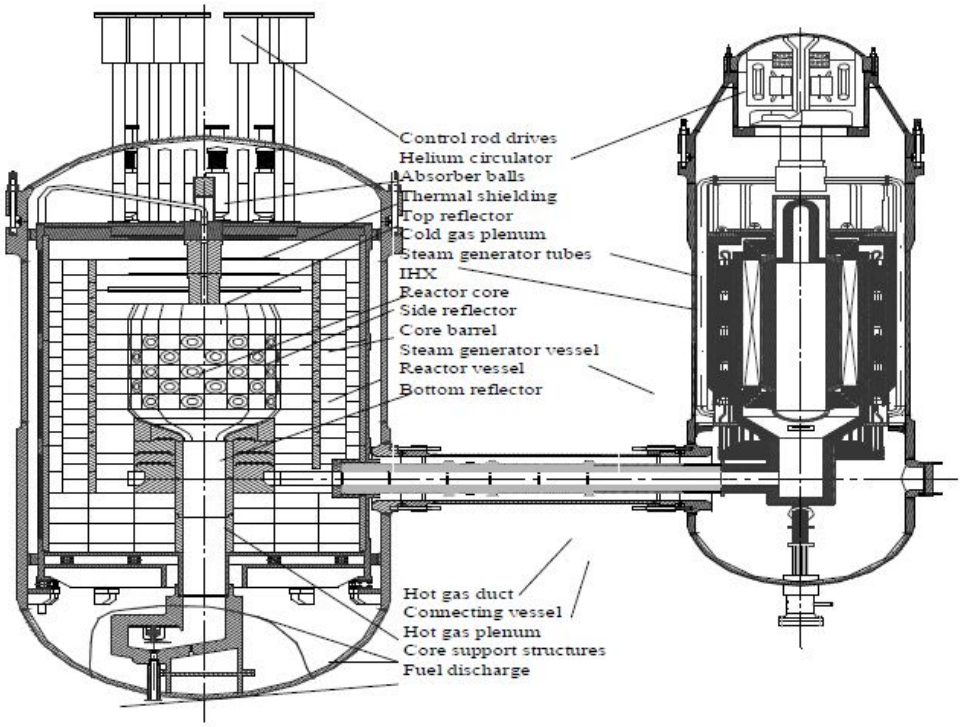

Fig. 1. Steam Generator Position on HTR-10 layout [14]

HTR-10 design is adopted from the design features of HTGR [15]. In general, the instrumentation of HTGR is not different from that of Pressurized Water Reactor (PWR). However, considering the position of the steam generator in the HTGR which is located on the primary circuit, it will have a little effect on the I&C requirements, because the secondary (water) side operating pressure is higher than the helium coolant pressure [13].

2.4. Computer-based for Instrumentation & Control System

I&C system of NPP consists of reactor protection system (RPS) and engineered safety features actuation system (ESFAS) as the common platform for safety critical I&C system. Based on this, the analysis of computer-based system is very important since RPS and ESFAS are consist of hardware, and software component [11, 16]. Modern I&C systems, generally consist of digital systems with the functions including software or hardware controlled by programming language, should be developed using life cycle model as safety critical aspects in NPP [17]. The development life cycle of digital I&C system are presented in **Fig. 2**.

In the development life cycle process, requirements analysis is the first thing should be completed before continuing to the next process. BAPETEN as national regulator, states that design of computer-based system related to safety for nuclear power should meet their criteria [18]. But since the requirements from BAPETEN did not state about the specific of reactors type, therefore BATAN as the applicant should review the international regulation as recommended by IAEA [2].

Detail of general requirements from IAEA which has the same contents with BAPETEN regulation No.6 year 2012 system design important to safety with computer-based system will be discussed in the requirements analysis.

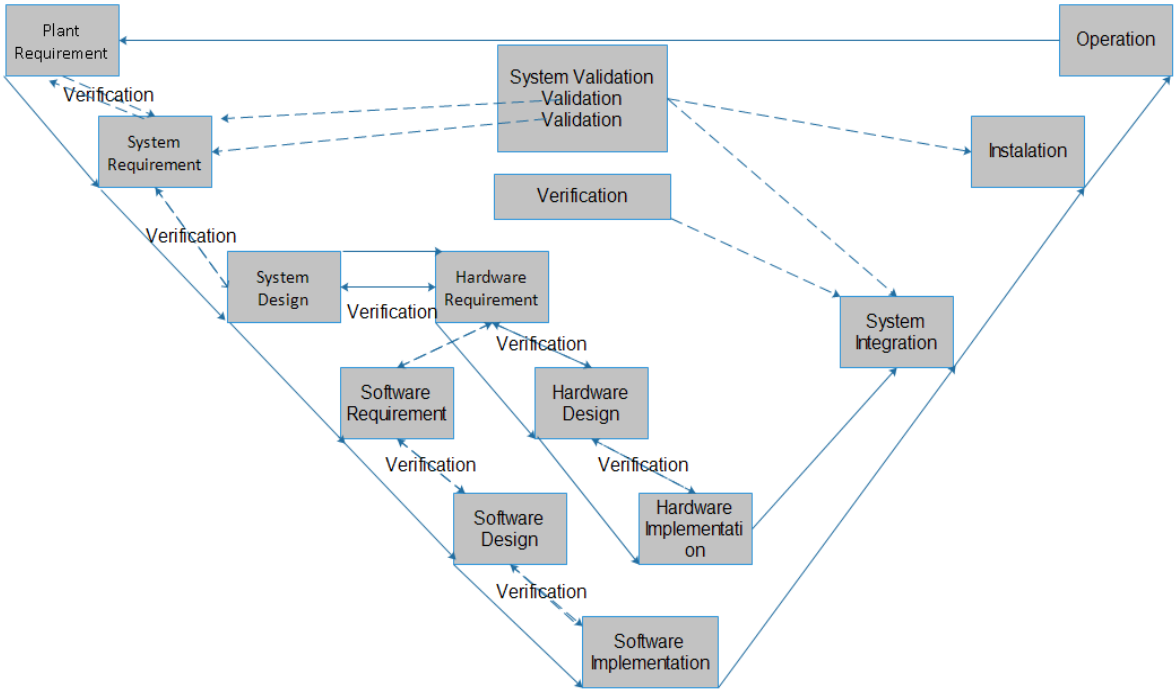

Fig. 2. I&C Development Life Cycle Process[17, 19]

3. METHODOLOGY

IAEA Specific Safety Guide (SSG) No.39 specifies that to ensure the safety of documentation and design bases related to the development of I&C with computer-based system, it should be controlled by life cycle process [17]. Standard Review Plan (SRP) Appendix 7.1 also provides that software life cycle has to be developed with the recommendation from RG1.173 which endorses IEEE Std 1074 as the standard for developing software life cycle processes [11]. Software requirements specifications (SRS) also need to review the digital testing plan of computer software [11, 20, 21]. Since the regulatory guide related to Non-LWR is still hard to find, and INET develop their own licensing applications [15], then Indonesia should develop licensing documents by completing analysis process to meet the criteria from the regulatory commission. Regulatory structure for development of HTR-10 in Indonesia and requirements traceability related to

development of computer-based I&C system for HTR-10 should be developed and analyzed in this paper.

Process for requirements analysis from the input which is collecting stakeholders requirements, and the design control documents from the regulator are presented in **Fig. 3** which produce requirements analysis documents using Icam Definition for Function Modeling (IDF0).

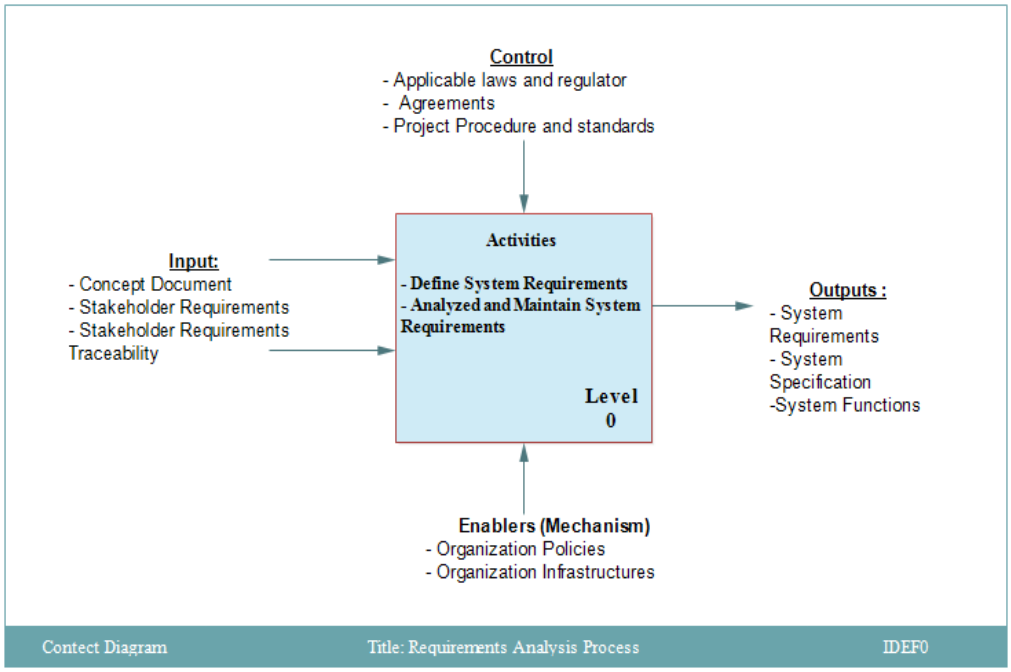

Fig. 3. IDEF0 Diagram for Methodology of Requirement Analysis Process

4. DISCUSSION

4.1 Relationship Regulatory Structure of Design Basis Document

Curently, Indonesia officially only has several guidelines regarding the design of power reactors from BAPETEN. **Fig. 4** represents the relation of utility requirements in coordination or comparing from international regulatory commission which is still have same requirements for the same system and components as the design basis documents for developing computer-based I&C system. GDC, BTP and RG have a role as the regulatory guide.

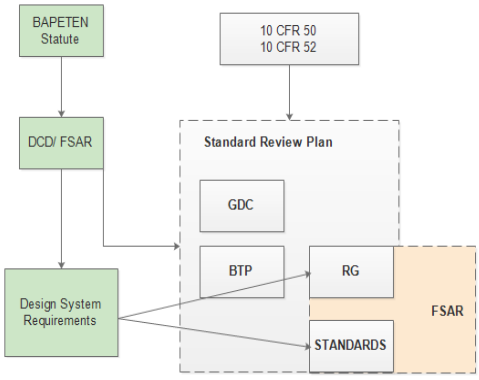

Fig. 4. Relation of Upstream Documents

The utility states the Design Control Document (DCD) to summarize all information related to RDE design als with Final Safety Analysis Report (FSAR) which provide information to support regulatory approval.

In addition to the design of computer-based system related to safety on power reactor, BAPETEN assigns the requirements that should be met. However, since BAPETEN did not specify the recommended codes and standards that should be taken, design engineer and the system analyst should compare them with the guidelines. In this case, document from IAEA can be used as reference since BAPETEN develops the law adopted from IAEA documents, therefore BATAN as the applicant of the licensing documents should make coordination with international regulatory commission [2]. Since USNRC as the global nuclear regulatoy commission, their documents can be used to compare the specific item which is important for process development to meet the design criteria of I&C system on NPP

4.2 Requirements Traceability

After collecting basic design documents, the codes and standars related to the design requirements can be tracked by developing requirement traceability. **Fig. 5** explains about the

top tier documents which is taken from the GDC of 10 CFR 50 Appendix A, Part 50.55 (a) and part 52.

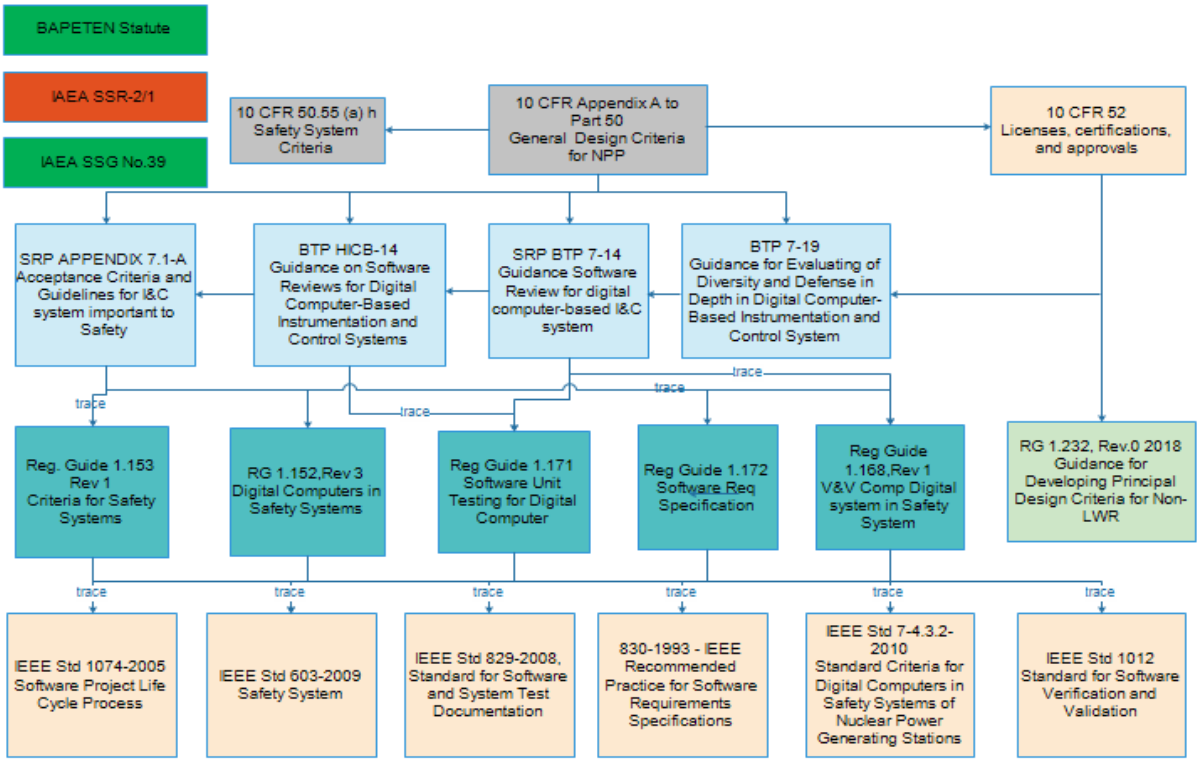

Fig. 5. Requirements Traceability Related to Computer-based I&C System

Requirements traceability diagram in **Fig. 5** explains that Nuclear Regulatory Commission (NRC) in 10 CFR for GDC, safety system and licensing part are discussed in this analysis which is related to the development of computer-based I&C system important to safety. Document of BTP and RG are positioned as regulatory requirements, acceptance criteria and guidelines which give recommendations to choose codes and standards related to I&C system.

4.3 Design Specification

Table 3 provides the specific requirements from document of IAEA SSG No.39 related to development of I&C System of NPP. In addition, **Table 3** only summarizes the design requirements related to computer-based development in I&C system.

Table 3. Requirements Analysis from the Design Specification of Computer-based I&C System[17]

Design Specification	Design Requirements	Guidelines	Standards	Requirement Type
Use life cycle model	The processes of the management system that are needed to achieve the goals, provide the means to meet all requirements and deliver the products of the organization shall be identified	Paragraph 5.1 of GS-R-3	IEEE Std 1074	Shall
Consideration of Common Cause Failure	The design of equipment shall take due account of the potential for common cause failures of items important to safety	Requirement 24 of SSR-2/1 (Rev. 1)		Shall
Safety Clasification of I&C Functions	The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices,	Requirement 18 of SSR-2/1 (Rev. 1)		Shall
Control of access to system important to safety	“Unauthorized access to computer hardware and software, shall be prevented.”.	SSR-2/1 (Rev.1) Requirement No. 39		Shall

Design Specification	Design Requirements	Guidelines	Standards	Requirement Type
Digital System	"If a system important to safety at the is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system."	SSR-2/1 (Rev.1) Requirement No. 63	IEEE Std 1074	Shall
deterministic response times	The design and analysis of digital systems should be such that failures of individual components.	SSR-2/1 (Rev.1) Requirement No. 61	IEEE Std 1012	Should
Computer security	"Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a NPP shall be designed and implemented in an integrated manner "	SSR-2/1 (Rev.1) Requirement No. 8		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,	SSR-2/1 (Rev.1) Requirement No. 63	IEEE Std 7-4.3.2^{TM} 2010	Shall
Software	Development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle.	SSR-2/1 (Rev.1) Requirement No. 63	IEEE Std 1074	Shall
Software Requirements	All software necessary to satisfy the I&C system requirements, including reused or automatically generated code, should have documented requirements	RG 1.172	IEEE 830	Should

Table 3 obtained from gathering important functions related to designing computer-based I & C systems important to safety from IAEA SSG No.39 which have similarities with the requirements requested by BAPETEN in regulation No.6 year 2012. The IAEA document SSG N0.39 also requires "shall" statement that should be met by the design applicant, together with the recommended standards.

5. CONCLUSION

Design engineer should decompose the functional components by developing the new functional analysis for HTR-10. After completing the requirement analysis, the analyst should characterize physical or functional attributes related to the system operation, measured or estimated under specified testing and operational environment conditions by synthesizing in to design architecture. The utility still has responsibility to complete the GDC for Non-LWR since this analysis are adopting the LWR documents with modification. This will be the future work for the design engineer to specify the design of Non-LWR especially for HTGR type.

ACKNOWLEDGMENT

Authors would like to thank Prof. Jae-Cheon Jung, Kepco International Nuclear Graduate School – South Korea, for his excellent guidance for requirement analysis for development of Instrumentation and Control System of Nuclear Power Plant. This research was supported by the 2018 Research Fund of the Center for Nuclear Reactor Technology and Safety – BATAN and Ministry of Research, Technology and Higher Education - INSINAS program 2018.

REFERENCES

1. Gou F., Chen F., Dong Y. Dynamic response of the HTR-10 under the control rod withdrawal test without scram. Energy Procedia. 2017. **127**:247–54.
2. IAEA *IAEA Nuclear Energy Series No.NP-T-1.13, Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants*. Iaea Nuclear Energy Series Publications. 2015.
3. Andrashov A., Bezsalyi V., Siora A., Sklyar V., Kovalenko A. Implementation of Digital Instrumentation and Control Systems for Nuclear Power Plant using FPGA - Technology : Benefits and Solution. in: *ReseLAS-ANS Symposium on Siting of new nuclear power and irradiated fuel facilities*. 2013. pp. 24–8.

4. IAEA *Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants, IAEA - TECDOC - 1327*. 2002.
5. Maerani R., Mayaka J.K., Jung J.C. Software Verification Process and Methodology for the Development of FPGA-based Engineered Safety Features System. Nucl. Eng. Des. 2018. **330**(April):325–31.
6. Yih S., Fan C.-F. Analyzing the Decision Making Process of Certifying Digital Control Systems of Nuclear Power Plants. Nucl. Eng. Des. 2012. **242**:379–88.
7. US.NRC *Guidance for Developing Principal Design Criteria for Non-Light Water Reactor, Regulatory Guice 1.232. Rev 0*. 2018.
8. Mcdowell B., Mitchell M., Pugh R., Nickolaus J., Swearingen G. *High Temperature Gas Reactors : Assessment of Applicable Codes and Standards*. U.S. Nuclear Regulatory Commission Regulations Pacific Northwest National Laboratory. 2011.
9. Theron W., Matzner D., Erasmus L. The Pebble Bed Modular Reactor and the Usage of Systems Engineering to Establish New Standards for the Nuclear Revival. in: *IFAC Proceedings Volumes (IFAC-PapersOnline)*. 2007. pp. 1–7.
10. Ball S.J., Cetiner M.S., Holcomb D.E. *Task 1 — Instrumentation in Vhtrs for Process Heat Applications*. 2010.
11. U.S.NRC *Standard Review Plan Appendix 7.1-A, Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety*. NUREG-75/087. 2005.
12. Jung J.C. Fundamentals of Systems Engineering, Requirements Analysis. in: *kepco International Nuclear Graduate School*. 2017.
13. S.J.Ball, Holcomb D.E., Cetiner S.M. HTGR Measurements and Instrumentation Systems. 2012.
14. Tyobeka B., Reitsma F. Results of the IAEA CRP5 - Benchmark Analysis Related To the PBMR-400, PBMM, GT-MHR, HTR-10 and the Astra Critical. in: *PHYSOR 2010 - Advances in Reactor Physics to Power the Nuclear Renaissance*. 2010.
15. Xu Y. The HTR-10 Project and its Further Development. Inst. Nucl. energy Technol. Tsinghua Univ. Beijing, China 1. 2000.(1):1–8.
16. Kumar L., Rajput H. Ensuring Safety in Design of Safety Critical Computer based Systems. Ann. Nucl. Energy. 2016. **92**:289–94.
17. IAEA *Safety Standards, Specific Safety Guide No.SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants*. 2016.
18. Bapeten *Peraturan Kepala Badan Pengawas Tenaga Nuklir Nomor 6 tahun 2012 tentang Desain Sistem yang Penting Untuk Keselamatan Berbasis Komputer pada Reaktor Daya*.
19. Maerani R., Saharudin, Sudarno, Santoso S., Deswandri, Bakhri S., et al. Developing Digital Instrumentation and Control System for Experimental Power Reactor by Following IEEE Std 1012 TM - 2004 to be Verified and Validated . in: *The 2nd International Conference on Energy Science (to be published)*. 2018.
20. Santoso S., Maerani R., Situmorang J., Cahyono A. Software requirement analysis for digital based reactor protection system of RDE design. in: *Symposium of Emerging Nuclear Technology and Engineering Novelty (to be published)*. 2018.
21. US. NRC Software Requirement Specification for Digital Computer Software and Complex Electronics Used in Safety System of Nuclear Power Plants. in: *Regulatory Guide 1.172*. 2013.