Software requirement analysis for digital based reactor protection system of RDE design

S. Santoso¹, Sudarno¹, R. Maerani¹, J. Situmorang¹, A. Cahyono²

¹Center for Nuclear Reactor Technology and Safety-BATAN, Puspiptek Complex, Building no.80, Serpong, Tangerang Selatan 15310, Indonesia
²Center for Engineering of Nuclear Facility-BATAN, Puspiptek Complex, Building no.71, Serpong, Tangerang Selatan 15310, Indonesia

Email: sigitsan@batan.go.id

Abstract. Experimental power reactor (RDE) is a helium gas cooled high temperature reactor which is under development and proposed to be constructed in Indonesia. To assure its safety and reliability many safety features are applied to this reactor design including the use of digital based I&C and Reactor Protection System (RPS). Reliability of the computer based RPS will depend on both hardware and software embedded in the system. Hence the impact of the applied software on reliability and safety must be considered. This paper discusses the process in determining software requirement specifications which is one of the important stages in a software development lifecycle. The requirement analysis process is conducted based on some standards such as IEC-60880, IEEE-1233 and IEEE-830. System Requirement Specifications (SyRS) and Software Requirement Specifications (SRS) for designed digital RPS software have been generated and defined in the analysis. Further analysis would be necessary to provide more detail information on SRS. The software requirements obtained in this study become essential information for conducting further activities in the software development of computer based RPS.

Keywords: RDE, software reliability, software requirements, RPS

1. Introduction
To meet the future national energy demands all potential energy resources including nuclear power should be considered properly. Hence the national technological capability, particularly in nuclear reactor technology becomes important. To cope with this issue a new type of research reactor called Experimental power reactor (RDE) which is mainly based on the high temperature gas cooled reactor technology is being developed. Comprehensive approaches were applied to the RDE design in order to enhance the safety and reliability [1]. In line to this purpose a digital based I&C was planned to be used in the RDE monitoring and control system. Moreover, the developed prototype design of the digital monitoring system and user interface such as an operator support system can also be adopted in the design process through a computer based simulator [2,3]. The digital I&C has been applied to many advanced reactor design such as ABWR, HTGR 10 MW and HTR-PM in China, FBR prototype in India, and others [4,5]. Application of the digital I&C systems provides many advantages such as better accuracy in control, more friendly human machine interface, and higher automation level, meanwhile there are also a challenge due to the reliability of embedded software [6-8].
The digital reactor protection system (RPS) was applied to the 10 MW high temperature gas cooled reactor designed and operated in China [6]. The function of RPS is generally to monitor and process variables essential to the safety of reactor and the environment, to detect accidents and automatically initiate protective actions. Protection system of RDE will be developed based on digital I&C technology and on the basis of the accident analysis. The design of digital I&C systems are different from the analog ones. For a particular case is the use of redundancy arrangement with multiple channels as applied for the analog RPS cannot be directly applied in digital systems. The digital component brings common cause failure (CCF) possibility which cannot be reduced by redundancy if the channels consist of the identical software and hardware [9,10].

When a protection system is controlled by a computer such as in a digital based RPS of nuclear reactor, the impact of the applied software on reliability and safety must be considered. To obtain a reliable and suitable software that control the reactor protection system, appropriate software development process should be determined. One of the important stage in the software development process is requirement analysis, which includes system requirement and software requirement. Preventing software defects can be realized by applying reliable software requirement in the problem representation [4,11]. Without appropriate and accurate requirements, the probability is high that some crucial concerns will be overlooked at some point in the next sequence of development phase.

This study aimed to generate software requirement specifications for the computer based digital RPS designed for RDE. This phase included in the requirement analysis of software development life cycle which consists of steps that provide a model for development and lifecycle management of software. The requirements analysis is based on the RDE design documents which is basic design and conceptual design document, and standards for software development, which are IEEE-1233 for the analysis of functional requirement specifications (FRS) and IEEE-830 for software requirements specifications (SRS) [1,12-14]. System requirements which should be fulfilled by software are brought into SRS document. To this time RPS of RDE is still being developed. Therefore discussion with RPS developer and reactor system developer is also carried out in this study to gain further depth information due to the RPS features and I&C components architecture which will be applied in the design. This paper describes the software requirement analysis applied to the digital based RPS design of RDE. Further analysis will be conducted following to the completion of the RPS design architecture in the development process. The results obtained in this study would be essentials for conducting appropriate software design process in order to obtain reliable and qualified RPS software.

2. Theory

2.1. Software Development Process

To obtain reliable and suitable software that controls the reactor protection system, appropriate software development plan and process should be applied. There is some guidance and criteria in the developing of software for safety critical I&C systems such as described in IEC 60880, 2006 as discussed in Chang et al.[9]. The development methodology consists of several main steps including requirement analysis, design phase, coding and testing. There are some standards that can be followed at each development phase. Based on this document, requirement analysis is separated into three phases which are System requirements specification (SyRS) or FRS, System architectural design and SRS.

The SyRS is analysed based on the design input document (operation and control note) of respective I&C systems, such as a reactor protection system. The purpose of the SyRS is to provide a black-box description of what the system should do, in terms of the system’s interactions or interfaces with its external environment. System requirements specification development is an iterative process. To conduct a full and accurate development of the SyRS, the decomposition of the process into sub processes and defined the sequential steps are required [14]. The four sub processes includes: a) Identify requirements from the customer/user, the environment, and the experience of the technical
community; b) Build well-formed requirements; c) Organize the requirements into an SyRS; d) Present the SyRS in various representations for different audiences.

During identify requirements the various inputs as presented in figure 1[14] should be filtered to be relevant with the system boundary. Some techniques can be applied in identifying requirements which includes interviews, observation of work pattern, simulations technical documents review, and others.

The SRS is a specification for a particular software product, program or set of programs that performs certain functions in a specific environment [13]. It should be defined by developer with considering inputs from user/customers. The basic issues to be considered in SRS construction are the functionality, what is the software supposed to do, external interfaces (how does the SW interact with people and system hardware), performance (what is the speed, response time of the systems/software functions, attributes such as portability, correctness, security considerations, and design constraint [13].

Information of the software requirement includes system interfaces, functional, performance and self-supervision requirements, constraints such as regulatory policies, hardware limitation, interface with other applications, language requirements, safety/security requirements and dependencies. Each functional requirement is detailed with purpose of the requirements, stimulus/response sequence and associated functionality to be carried out. In order to satisfy the good characteristics of SRS it should be correct, unambiguous, consistent, verifiable and traceable.

![Figure 1. Context for developing of System requirement specifications [14]](image)

2.2. I&C of Experimental Power Reactor (RDE)
The instrumentation and control equipment of RDE is divided into operational systems, limitation systems, protection systems and accident monitoring systems [1]. According to the protection system, the digital based RPS for RDE would be applied to generate the reactor trip signal and the engineered safety features actuation signal in case of design basis accidents. There are many advantages by applying digital system on RPS such as, small size for the equipments, decrease in components, reduction of connection lines due to network techniques, stability and high precision for the set points.

The RPS is independent from the analog data acquisition equipment through to the actuation equipment for: reflector rods, Primary gas blower, Primary system isolation valves, Secondary system isolation valves, and Steam generator relief valves. The reactor protection system is designed in such a way that it can fulfill its safety function even when failure initiating events occur within the reactor protection system or within the reactor system. The circuitry of the reactor protection system is divided into three sections, that are Initiation level, logic level and actuation level. The initiation level of the RPS comprises a data acquisition from the sensors through to the limit value monitors. Logic level responsible in the generation of limit signal, voting and gating logics of limit signals to produce actuation signals. The last level of protection system which is actuation level responsible in conducting a process of actuation signals from the logic level to actuate safety equipment. The logic level of RPS design in general is presented in figure 2.
3. Methodology
Analysis of software requirement embedded in the digital RPS design for RDE was conducted based on the reactor design documents which are basic design and conceptual design of I&C, and standards for software development which is IEEE-1233 for analysis of functional requirement specifications (FRS/SyRS) and IEEE-830 for software requirements specifications (SRS). Discussion with RPS designer and user was performed in order to cultivate the system requirement and need, and to gain information on architecture design of RPS components and implemented features. Requirement analysis of RPS software was conducted in the two following steps: The first step is to define the SyRS for the reactor protection system in general and FRS/SyRS for each RPS sub-system including initiation level, logic level, and actuation level based on the design input documents of respective I&C systems. The second step is conducting analysis based on the cultivated SyRS and IEEE std. 830 to identify and formulate the software requirement specifications for general system, and particularly for each RPS sub-system.

4. Result and discussion
4.1. Functional requirement of SyRS
Analysis of the system requirements specifications were conducted for general system, and specifically for each of the RPS circuitries as well. Separation of RPS into sub systems based on the process level sequence would be useful in developing of modular software and in conducting verification and validation process. Identification of functional requirements for the system requirements specifications (SyRS) of digital RPS of RDE is summarized in Table 1. This requirement is extracted based on the function, design features, the required input/output of protection system/sub system of RDE and other related systems while the analysis process was based on the IEEE-1233 standard.

The FRS/SyRS of RPS software is essential for ensuring that the defined system function would be satisfied. Presented in Table 1, there are five general requirements identified in the current RPS
development stage. These requirements can be changed and modified during the development process according to the system architecture design change or additional functions applied to RPS. Process sub system of digital RPS which is divided into three levels module should also satisfy the functional requirements of each level.

Dealing with the functional requirements of SyRS as is showed in Table 1, RPS of RDE should be supported with an appropriate environment system such as associated digital functions which cover a relay logic, timing and sequencing, and display for input and output status. Reliability of processor modul and its process memory, appropriateness of applied real time clock resolution, and continuous support from market/vendor on applied hardware need to be considered in the RPS design. Moreover, compared to other control systems applied to reactor, the RPS should be designed with highest level in reliability and security of operations.

Table 1. Functional requirements for the SyRS of RDE-RPS

| No | Process sub-system of digital RPS | Functional requirements |
|----|-----------------------------------|-------------------------|
| 1  | General                           | - If one of the reactor scram initiating criteria is fulfilled, the reactor protection system is designed to initiate sequences of appropriate scram actions  
- The protection system is designed to override manual actions and open and closed loop controls which is aimed to ensure the safety of personnel, environment and the entire plant facilities.  
- The reactor protective system detects safety-related plant state variables, processes them and initiates the appropriate actions.  
- The equipment unit protection system contains the high-grade protection circuits for important equipment units and the protective interlocks for all equipment units.  
- In each RPS channel, only signal processing devices and logic voting devices are designed in digital format. |
| 2  | Initiation level module           | - Comprise a data acquisition from the sensors through to the limit value monitors.  
- Convert analog input signal to the digital form prior further transmitted to digital processor  
- The initiation channels are continuously monitored by analog comparators for malfunction. |
| 3  | Logic level module                | - Generate set point signal for initiating criteria, conduct voting logic and gating logic based on signal input and reference limit. Monitor reference limit in the initiation channels.  
- Determined by the generation of limit signals for the initiation criteria, the logic voting (e.g. 2-of-3) of the redundant limit signals and the logic gating of the |
initiation criteria
- Process all received signal appropriately as presented in the designed logic diagram. Trip signal should be generated and sent to the actuation unit

4. Actuation level module
- Convert the actuation signals from the logic level into trip signals to activate corresponding protection equipment at the actuation level.
- Provide interlock in order to protect the trip actions execution using different mode simultaneously.
- Provision is made for the simulation of actuation signals for testing the actuation level and the safety features to which it is connected.

| No | Process sub-system of digital RPS | Requirements specification |
|----|---------------------------------|----------------------------|
| 1. | General                         | - Applied diversity such as by provided a design with at least two different channels that uses diverse digital system.  
   |                                 | - The embedded software should not generate the unnecessary complexity to the system.  
   |                                 | - The designed RPS software should consider on some aspects such as the system required response time, fault tolerance, availability, and maintainability factor. |
| 2. | Initiation level module         | **Inputs:** nine of analog inputs includes intermediate and power range neutron flux, hot and cold gas temperature, primary coolant mass flow, feed water mass flow, primary system pressure, moisture in primary system and pressure in secondary system should be scanned from analog input card.  
   |                                 | **Outputs:** all analog signal are converted to digital form  
   |                                 | **Processing logic:** check and compare the converted digital signal to the reference limit to generate protection initiating signal. Provide data for visualization and recording system. |
| 3. | Logic level Unit                | **Inputs:** digital signal output from initiation level module  
   |                                 | **Outputs:** digital signal output represents the result from voting and gating process.  
   |                                 | **Processing logic:** Voting and gating the signal based on the initiation criteria of applied gating logic and trip scenarios. |
4. Actuation level module

**Inputs:** digital signal actuation from logic unit

**Outputs:** digital signal trip.

**Processing logic:** generate actuation signal for reactor scram which is appropriate to the trip scenario. Generate relay output when any two of the three logic signals are satisfied.

4.2. Functional requirements of SRS

Software Req. Spec. includes analysis and documentation of requirements. The analysis result is presented in Table 2, which shows the functional requirements of SRS that should be fulfilled in the software designed for RPS-RDE. As shown in Table 2, developing the software for safety critical system generally should apply diversity concept in the design. Implementation of software design from different manufactures or platform on the different channels can be used to achieve this purpose. Separation of the software into some software modules can also be applied on the RPS software design in order to increase maintainability, flexibility and to reduce its complexity. During the process development the use of compact modular software will be suitable in order to anticipate the frequently feature changes of the system. Other significant aspect in time critical systems like RPS of RDE is a high response time which should be met with the requirement. Specifically, the system needs to satisfy both functional requirements and performance requirements such as fault tolerance, time response, and system availability.

To this time Reactor protection system for RDE is under development process and the final RPS design is not yet defined. Hence, there are still some options available and considered to be implemented in the RPS system. The development of RPS software is an iterative process which also depend on the hardware architecture and I&C components. The SRS could be updated and developed in more detail in line with the design development process and availability of corresponding detail design data. It is essential since the SyRS and SRS obtained in the requirement analysis would be used in the software design phase. Design development organization is responsible for developing, maintaining, and updating SRS.

5. Conclusion

Requirements analysis is an important stage in the software development life cycle of RDE-RPS since most software error was initiated from this phase. Analysis of System requirement specification and Software requirement specification were conducted in the design process of protection system of RDE based on the design documents, standard and criteria for software design on critical systems. The SyRS and SRS for software embedded in the RPS design have been generated and formulated in this study. The analysis result showed that in order to attain reliable RPS software the identified SRS should be satisfied in the design. This includes the implementation of diversity by providing the design with at least two different channels of diverse digital systems, avoid unnecessary complexity, consider to the response time, fault tolerance, and maintainability factor. Moreover, modularization of RPS embedded software based on the specific function of RPS sub-system, such as initiation process level, logic process level, and actuation level would be required in reducing complexity and enhancing maintainability of the software.

6. Acknowledgements

This research was a part of research project supported and funded by the Nuclear Research & Development Program (DIPA 2018) at the Center for Nuclear Reactor Technology and Safety of the
National Nuclear Energy Agency, and research grant from Ministry of High Education and Science Technology of Indonesia FY 2018.

References
[1] Brinkmann G, 2015 “Intermediate Report: Conceptual Design of Instrumentation and Control Equipment,” DS-WBS02-215, KOGAS, NUKEM Technologies, dan Rekayasa Engineering
[2] Liu P, Li Z, 2016 Int. Journal of Industrial Ergonomics. 51, 2-9.
[3] Santoso S, Situmorang J, Bakhri S, et al 2018, IOP Conf. Series: Journal of Physics: Conf. Series 962 (2018) 012006
[4] Guo C, Xiong H, Huang X, et al., 2017 J. Sci. and Technol of Nucl. Install. 2017, 1-9
[5] Manimaran M., Shanmugam A., Parimalam, P., et al., 2014 J. Nucl. Eng. Des. 268, 96–103.
[6] Yoshikawa H, 2013 J. Nuclear Eng. and Technol. 45(2) 165-178
[7] Yastrebenetsky M and Kharchenko V, 2016 “Reliability and safety of nuclear power plant instrumentation and control systems: New challenges and solutions,” in Proceedings of the 2nd International Symposium on Stochastic Models in Reliability Engineering, Life Science, and Operations Management (SMRLO ’16), pp. 47–55, February 2016.
[8] Zou B, Yang M, Benjamin E.R, et al., 2017 Progress in Nuclear Energy 98 85-93
[9] Cheng Y, Chao N, Tian Z., et al., 2014 Prog. Nucl. Energy. 70, 128–133
[10] Ma Z, Yoshikawa H., Yang M, 2017 Annals of Nuclear Energy. 110, 805-817
[11] Huang F., Liu B, 2017 Chinese Journal of Aeronautics, 30(3) 1054-1070.
[12] Park G.Y, Jang S.C. 2014 Nucl Eng and Technol 44(1) 55-62
[13] IEEE Std. 830, 1998a. IEEE Recommended Practice for Software Requirements Specifications. 1998
[14] IEEE Std. 1233, 1998c. IEEE Guide for Developing System Requirements Specifications, 1998