Assessment of Input Parameters and Architecture of RDE Reactor Protection System

Sudarno, Sigit Santoso, Kussigit Santosa, Restu Maerani, Deswandri
Center for Nuclear Reactor Technology and Safety – BATAN,
Puspiptek Area Building 80, Serpong, South Tangerang City, 15310, INDONESIA

Email: sudarno@batan.go.id

Abstract. The Experimental Power Reactor (RDE) is a High Temperature Gas Cooled Reactor (HTGR) with 10 MW thermal which is planned as the first nuclear power plant (NPP) in Indonesia. The purpose of RDE development for Indonesia is to become technology provider related to the provision of electrical energy and cogeneration and become superior in the region. The safety factor is the most important factor in the operation of nuclear reactor to maintain the safety of reactor, people and the environment. Reactor Protection System (RPS) is an instrumentation and control system that serves to ensure the safety of the operation of the reactor, which will perform the reactor trip automatically if the reactor operation exceeds the safety limits. The research of RDE RPS design aims to support the development activities of RDE detailed design especially in RPS design. This design is based on accidents already outlined in Design Basic Accident (DBA) and is designed with a level of reliability that meets the requirements. In order for RPS to function when demanded it is necessary to know the parameters of the process used for the detection of the occurrence of DBA. The purpose of this research is to identify the input parameters used by RPS especially at the initiating level. The results of the identification obtained are important in the development of RPS architecture. The research methodology was conducted with DBA scenario analysis listed in the RDE conceptual design document and RPS design review on HTGR in general.

Keywords: Input parameter, architecture, RDE, Reactor protection System

1. Introduction
The Experimental Power Reactor (RDE) is a High Temperature Gas Cooled Reactor (HTGR) with 10 MW thermal which is planned as the first nuclear power plant (NPP) in Indonesia. The purpose of RDE development for Indonesia is to become technology provider related to the provision of electrical energy and cogeneration and become superior in the region. In the long term, the RDE is a milestone of the mastery of commercial NPP technology. In 2015 RDE conceptual design has been completed, followed by basic design. In 2018 RDE detailed design is performed as the next stage of RDE development program[1].

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd
The safety factor is the most important factor in the operation of nuclear reactor to maintain the safety of reactors, people and the environment. RPS is an instrumentation and control system that serves to ensure the safety of the operation of the reactor, which will perform the reactor trip automatically if the reactor operation exceeds the safety limits. The RDE RPS design uses digital technology and takes into account the standards of nuclear reactor safety systems. The digital RPS provides a series of advantages such as better accuracy of monitor and control, more friendly human-machine interface, and higher automation level [2,3,4]. However, the RPS digital reliability factor, especially the software reliability is still a research topic in evolvement[5,6,7].

The research of RDE RPS aims to support the development activities of RDE detailed design especially in RPS design. The RPS function is to monitor and process variables essential to the safety of reactors and the environment, to detect accidents and automatically initiate protective actions. The choice of monitored process variables, derivation of appropriate initiative criteria and the generation of actuation signals for protective actions are performed on the basis of the accident analyses. The RPS design is based on accidents already outlined in Design Basic Accident (DBA) and is designed with a level of reliability that meets the requirements. In order for RPS to function when demanded it is necessary to know the parameters of the process used for the detection of the occurrence of DBA [8,9,10]. The purpose of this research is to identify the input parameters used by RPS especially at the initiating level. The results of the identification obtained are important in the development of RPS architecture. The research methodology was conducted with DBA scenario analysis listed in the RDE conceptual design document and RPS design review on HTGR reactor in general.

2. Theory

Criteria of Instrumentation and Control for Safety System
The design of the digital instrumentation system as part of the safety system shall take into account the criteria for the safety system. In accordance with the IEEE 603-2009 standard on "Criteria for Safety Systems for Nuclear Power Generating Stations", the safety system must have certain precision and reliability to keep the reactor operating parameters within acceptable limits for each. The criteria to be met by the safety system are[11]:

- Single failure.
  Single failure can occur before or during DBA, where the safety system is needed to function. Single failure criteria apply to safety systems either automatically or manually. The application of single failure criteria may refer to the IEEE 379-2000 standard [12].

-Completeness of protective measures.
  The safety system must be designed so that, once activated either automatically or manually, the sequence of protective actions will take place until it is complete. Thereafter, to restore the safety system to normal condition requires operator action.

- Quality.
  Components and modules must meet quality consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated and maintained in accordance with the quality assurance program established for such components or modules.

- Equipment qualification.
  The safety system equipment shall be qualified by the type of test, operating experience already undertaken, analysis or combination of these three, to meet performance as required in the design basis.

- System integrity
  The safety system shall be designed to meet the safety functions within the whole range of the conditions specified in the design basis.

- Independence
- Redundant parts of the safety system shall be independent (physically separate) from each other in such a way that the safety functions are met during and after DBA.
- The safety system equipment required to mitigate the consequences of a particular DBA must be independent of the effects of DBA.
- The design of the safety system shall be independent of other safety systems, so failure or consequence of such other safety systems does not interfere with the fulfillment of safety functions.

• Ability for testing and calibration
  The capability for testing and calibration of safety system equipment should be available, without interfering with the system's ability to perform safety functions. Testing and calibration can be performed during reactor power operation.

• Display Information
  - Instrumentation of displays for actions that are only controlled manually, and to perform the safety functions, shall be part of the safety system, and shall comply with the IEEE 497-2002 standards.
  - Instrumentation of the display must provide an accurate, complete and timely information of the state of the safety system.
  - If the part of the safety system for protective action is bypassed, then the information should be displayed in the control room continuously.
  - Display information must be in a place that the operator can access. Information required by the operator to perform the action manually should be visible from the operator's location to perform the manual action.

• Access control
  The design of the safety system should allow the control of administrative access to safety system equipment.

• Improvements
  Safety systems should be designed to facilitate the detection, replacement and repair of malfunctioning equipment.

• Identification
  To ensure that the requirements in the standard are met in the design, construction, operation and maintenance stages of the nuclear power plant, identification should be easy for equipment safety systems, components, modules, computer hardware and software and related documents.

• Additional features
  Additional features are features that do not execute protective actions like a trip system, but support for the safety functionality to work properly. Examples of these additional features such as HVAC systems, generators, transformers etc. The design of these additional support features shall meet the requirements of the standard.

• Multi-unit stations
  The structures, systems, components shared among units on a multi-unit nuclear power plant are allowed as long as they do not interfere with safety functions in all units. Guidelines for joint use of electrical power systems as set out in the IEEE 308-2001 standard.

• Human factor considerations
  Human factors should be considered during the design process to ensure operators and maintenance workers can perform their duties properly.

• Reliability
  Reliability analysis of the safety system design needs to be done to be able to confirm that the guarantee of fulfilling the safety function is met. Reliability analysis can use both quantitative and qualitative methods.

• Common cause
Common cause evaluation is necessary for components and systems, both hardware and software. Common cause is indispensable in calculating system reliability.

3. Methodology
Assessment of input parameters for design of RDE RPS is done by analyzing postulated accidents that are included in the RDE DBA. From accident scenarios, safety parameters involved in each DBA are determined. Assessment of RDE RPS architecture is done by identifying RPS functions, inputs and outputs as well as RPS components. The expected RPS architecture is a block diagram of the RPS and its descriptions.

4. Results and Discussion
RPS will maintain the safety of reactor operation by performing a trip reactor especially at the time of DBA incident. The initiation criteria provided in the reactor protection system for RDE and the consequences of protective actions are summarized in the following categories:

- Reactivity accidents
- Loss of flow events in the primary and secondary system
- Primary system depressurization
- Steam generator tube breaks
- Earthquake

The protective actions thus initiated are:

- Reflector rod drop
- Primary helium gas blower trip
- Isolation of the steam generator, main steam and feedwater lines
- Isolation of primary system
- Steam generator relief

The first three protective actions in the list (as known as module trip) are initiated in response to all initiating criteria. Additionally initiated protective actions are:

- Primary system isolation for the primary system depressurization accident category, and
- Steam generator relief for the tube leakage accident category.

4.1 Reactivity accidents
Reactivity accidents can occur at startup operations, full power or power reactor changes. This accident category is detected on the basis of initiation criteria derived from the process variables neutron flux or hot gas temperature.

Module trip in the event of reactivity accidents during start-up is actuated either in response to the initiating criterion

- Thermal neutron flux more than approx. 120 %, or to both limits of the initiating criterion
- Intermediate-range neutron flux more than maximum
- Period less than approx. 20 s

The three protective actions (i.e. reflector rod drop, primary helium gas blower trip, and isolation secondary system) leading to module trip change the plant to a safe condition.

4.2 Loss-of-flow events
The LOFA event will cause the heat transfer capability of the reactor core to be reduced. This accident category is generally associated with the mass flow system, the initiating criterion which can be used for such events

- Mass flow ratio (primary to secondary side) is more than 1.3 or less than 0.75

For secondary-side breaks, module trip can be initiated in response to the initiating criterion:

- Cold gas temperature more than 280 °C
- Negative sliding limit value of main steam pressure higher or equal to 8 bar / min

The mass flow signal is adjusted to the feedwater pump or the primary gas blower (e.g. during changeover operations of the feedwater pump) do not cause trip.
4.3 Depressurization accident
Depressurization accident can result in overheating of the reactor pressure vessel. To reduce the consequences of accidents in this category, the main trip module is actuated, besides the RPS will also initiate action:
- Primary system isolation
  This isolation prevents further fluid loss from the primary system through each break downstream of the primary system isolation valve. This action was initiated in response to the initiation criteria:
  - Negative shear limit for primary system pressure over 180 mbar / min
    The limit settings are chosen such that the response does not occur as a result of operational malfunctions, such as pressure control failures, and during shutdown operations.
  - The mass flow ratio (primary to secondary side) is less than 0.75

4.4 Steam generator tube leakages
Tube leakage is always connected with the ingress of water or vapor into the primary system. To limit leakage that exceeds operationally acceptable level in the event of leakage, the trip module is actuated in response to the initiation criteria specific to these accidents.
- Moisture in primary system higher or equal to 800 vpm
  moreover the following action is also initiated:
  - Steam generator relief
    Depressurization from the primary side is prevented by the valve which close automatically by spring resistance in case of pressure balance of primary and secondary sides.

4.5 Earthquake
The seismic instrumentation system of the RDE is to record and measure seismic activity in the reactor building and the area around the site. Instrumentation gives an indication of ground motion and records it to analyze seismic history. To ensure the recording of seismic activity, the recording system consists of two redundant systems. If the acceleration limit specified in the design is exceeded, the reactor protection system actuates the main trip module.

From the previous DBA analysis, a postulated initiating event is detected if there is one or more process variables that have values beyond the safety margin. Variables related to initiating events are called initiating criteria. Table 1 provides a list of parameters and measuring points to measure the value of those variables.

| Process variable                      | Measuring range (approximate data) |
|--------------------------------------|------------------------------------|
| Intermediate-range neutron flux      | $5 \times 10^2$ ... $5 \times 10^6$ cm$^2$s$^{-1}$ |
| Power-range neutron flux             | $5 \times 10^6$ ... $5 \times 10^8$ cm$^2$s$^{-1}$ |
| Hot gas temperature                  | 0 ... 850 °C                      |
| Cold gas temperature                 | 0 ... 350 °C                      |
| Primary coolant mass flow            | 0 ... 100 kg/s                    |
| Feedwater mass flow                  | 0 ... 100 kg/s                    |
| Primary system pressure              | 0 ... 80 bar                      |
| Moisture in primary system           | 100 ... 1000 vpm                  |
| Pressure in secondary system         | 50 ... 230 bar                    |
4.6 RPS Architecture

RPS has functions: bistable, coincidence logic, initiation trip circuit and maintenance / test functions. The circuitry of the reactor protection system is divided into three sections:

- **Initiation level**, The initiation level of the RPS includes the acquisition data from the sensor to the limit value monitor. Process variables in each initiation channel group are acquired in triplicate and are gated in 2-of-3 voting circuits. One exception is a one-of-two voting circuit for medium-range neutron flux instrumentation. The sensor transmitter output signal is converted into an analog current signal in the transducer compartment. The neutron flux instrumentation is an exception where the current signal is generated in the instrumentation cabinet and passed directly to the analog section with exception the intermediate range required for the remote shutdown station.

- **Logic level** This level includes the generation of limit signals for the initiation criteria, the logic selection (i.e., 2-of-3) of the redundant limit signals and the gating logic of the initiation criteria to produce actuation signals. The Local Coincidence Logic (LCL) Processor Module is a logical signal processing using voting logic 2-out-of-3. This module receives trip signal input from bistable and bypass signal signals from Maintenance and Test Panel (MTP). The LCL module consists of: Processor Modules (PM), Communication Interface Module (CI), Digital Input Modules (DI), Digital Output Modules (DO), and Analog Output Modules (AO). To prevent a fault in one trip channel from scramming the reactor, the output signals from the redundant trip channels are again 2-of-3 gated with each other in three voting circuits before the redundant actuation signals for the protective action are passed to the actuation level.

- **Actuation level** The actuation signal from the logic level is converted into a trip signal for active protection equipment. It is divided into three redundant subsystems. The drop of the reflector rod is initiated by breaking the holding current at both poles of the rod drive mechanism with a 2-of-3 gate combination of two sets of three relays. The primary helium blower trip is effected redundantly by two circuit breakers in series and additionally by blocking the thyristors in motor control. The steam generator isolation is carried out by the redundant opening of two circuit breakers of each isolation valve that interrupt the current holding the pilot valve. This pilot valve eases the pilot pressure from the feedwater and mainsteam insulation valves. This results in the closure of the feedwater and mainsteam isolation valves. The steam generator relief is carried out by opening the redundant two circuit breakers of each isolation valve that interrupt the flow of the pilot valve. This pilot valve reduces pilot pressure. This results in the opening of this isolation valve.

RPS architecture consists of 3 redundant channels, one RPS channel diagram can be seen in Figure 1.
4.7 Logical Functions Bistable

The Bistable Processor (BP) on each channel receives an analog signal input from sensors and digital signals from the Calculator Processor. BP will compare the value of input parameters with trip set point, to detect the presence of input parameters that cause trip reactor. Set point BP needs to pay attention to setpoint functions based on its input parameters:

- Bistable with constant setpoint (digital).
  Changing constant setting point value can be done on RPS.
- Bistable with setpoint variable.
  Setpoint variables are provided for safe operation at start up and shut down.
- Setpoint variable with manual reset.
  This setpoint variable type allows automatic decrement of setpoint values manually manipulated using the RPS operator module in the Main Control Room or manual reset switch. Decrease in setpoint value is a function of input signal to bistable. For example on the pressure ratio parameter between the primary and secondary systems. In this case the primary system pressure can be used as the input parameter to determine the set point of the secondary system.

Because the set point used can be either constant or variable, therefore in the design of the comparator algorithm of BP needs to consider the set point types for each parameter input.

5. Conclusion

An assessment of input parameters of RDE RPS has been conducted, by analyzing postulated accidents included in the RDE DBA. RPS input parameters consist of analog signals from sensor-transducer and digital signals from Calculator Processor. The RDE RPS design uses RPS digital technology, consisting of 3 redundant channels to meet the required level of RPS reliability. The series of each channel is arranged in three levels: initiation level, logic level, and actuation level.

6. Acknowledgments

The research was funded by the INSINAS-FLAGSHIP RDE Grant of the Indonesian Ministry of Technology and Higher Education of 2018 fiscal year.
References

[1] Tim BEDP-RDE BATAN. 2017. “Dokumen Input Desain RDE, Basic Engineering Design of Reaktor Daya Eksperimental”, September 2017

[2] M. Yastrebenetsky and V. Kharchenko, “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.

[3] Sudarno, "Analisis Keandalan Sistem Proteksi Reaktor PWR", Prosiding Seminar Nasional ke-13 Teknologi dan Keselamatan PLTN Serta Fasilitas Nuklir, ISSN: 0854-2910., 2007

[4] Sudarno, “Evaluasi Keandalan Sistem Instrumentasi Digital Pada Sistem Keselamatan PLTN”, Prosiding Seminar Nasional TKPFN ke-17, Yogyakarta, Oktober 2011.

[5] "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE 7-4.3.2-2003

[6] X. Li, M. Xie, and S. H. Ng, “Sensitivity analysis of release time of software reliability models incorporating testing effort with multiple change-points,” Applied Mathematical Modelling. Simulation and Computation for Engineering and Environmental Systems, vol. 34, no. 11, pp. 3560–3570, 2010.

[7] Guo, C., Xiong, H., Huang, X., & Li, D. (2017). Design and Development Framework of Safety-Critical Software in HTR-PM, 2017. Hindawi Science and Technology of Nuclear Installations Volume 2017.

[8] Fu Li, Zijue Yang, Zhencai An, Liangju Zhang, “The first digital reactor protection system in China”, Nuclear Engineering and Design 218 (2002) 215–225

[9] Liu Hongchun, Wang Huajin, Zhou Jixiang, Xu Dongfang, Wang Taotao, & Liu Guangming Design of digital reactor protection system of Ling’ao Phase II NPP. Nuclear Power Engineering, 29(1), 1-49 (2008).

[10] Verrastro, C. A., Estryk, D. S., Rodriguez, G. F., Ferrucci, F. N., Alarcón, J. E., Ríos, G. E., & Lee, J. J. (2014). FPGA Based Reactor Protection System Architecture. Comision Nacional de Energia Atomica.

[11] "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", IEEE 603-2009

[12] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”, IEEE Std 379-2000 (R2008).