THE DIGITAL REACTOR PROTECTION SYSTEM FOR THE INSTRUMENTATION AND CONTROL OF REAKTOR TRIGA PUSPATI (RTP).

Nurfarhana Ayuni Joha, Izhar Abu Hussin, Mohd Idris Taib,
Zareen Khan Abdul Jalil Khan
Electronic, Instrumentation and Control section
Nuclear Power Division
Malaysian Nuclear Agency

Abstract

Reactor Protection System (RPS) is important for Reactor Instrumentation and Control System. The RPS comprises all redundant electrical devices and circuitry involved in the generation of those initiating signals associated to the trip protective function. The instrumentation system for the RPS provides automatic protection signals against unsafe and improper reactor operation. The physical separation is provided for all of the redundant instrumentation systems to preserve redundancy. The safety protection systems using circuits composed of analog instruments and relays with relay contacts is difficult to realize from various reasons. Therefore, an application of digital technology can be said a logical conclusion also in the light of its functional superiority.

Keywords: Reactor Protection System, High Power Channel, Fuel temperature channel, high voltage power supply, Reactor Monitoring System

INTRODUCTION

The I&C systems of RTP were manufactured and supplied by the TRIGA manufacturer General Atomic of United States. All electronic circuit boards are fabricated with shape such that they can be slotted into their correct place only. This will avoid any un-deterministic condition to the system or damage to the board when repair or replacement jobs are carried out. The main inherent safety feature of the I&C system design is such that any failure in the electronic or its associated components, does not lead to an uncontrolled rate of reactivity.

RTP I&C system provides a means of protecting the reactor from undue conditions or abnormal circumstances that could result in an accident. In case of any abnormality, the protection logic will generate a power SCRAM signal that releases all control rods into the core.

All functions essential to operation of the reactor are controlled by the operator from a desk-type control console that contains the electronics of the instrumentation and control systems. Instrumentations contained in the console are connected to the detectors around the reactor core as well as the control rod drives, by means of special interlock system for safety and protection.

The majority of research reactors operating today were put into operation some 20 years ago, some of them undergone modifications and refurbishing since their construction and many have been upgraded in power to meet requirements for higher neutron fluxes with or without any changes to their I & C systems. A number of old reactors are still operating with some parts and components of the original system. Old I&C systems cause operational problems as well as difficulties in obtaining replacement parts. In addition, there are the increasing demands of safety requirements.

Technical advances in I & C systems have been rapid in the past years, and this technology should be adapted by the research reactor community. The introduction of improved safety instrumentation on existing and future nuclear facilities is a continuous and evolving process. For the old facilities, the main objective is to provide improved systems to be consistent with modern safety standards, to cope with equipment obsolesce and to permit improved economical parameters.

Several technical requirements must be fulfilled while making any modifications or modernization of I&C systems. These are:

- safety requirements,
- operational requirements,
- budget constrains (including minimization of outage time).

The safe, reliable and economical operation of existing research reactors must be ensured and therefore, careful consideration must be given to the modernization of the old I & C systems.

REACTOR PROTECTION SYSTEM

Definition

The Reactor Protection System encloses all electrical and mechanical devices and circuitry involved in generating the initiation signals associated with protective functions that are carry out by the Safety Actuation Systems.

The Reactor Protection System (RPS) is a very important system in a research reactor because the system shuts down the reactor to maintain the reactor core integrity and the reactor coolant system pressure boundary if the operation conditions approach the specified safety limits. To assure the safe operation of a reactor, the RPS is designed according to the redundancy criteria to prevent a single failure. The 1-out-of-2 RPS system consists of two channels, and each channel is implemented with the same architecture. The reactor will be in an unsafe state when the RPS does not generate the reactor trip signal on demand. If the RPS is operating correctly, it can shut down the reactor anytime on demand. In this case, the reactor safety requirement is satisfied. If any failure happens in the RPS and it is detected by the system, the RPS automatically generates the channel trip signal according to the fail safe requirement of the RPS [3]. From a reliability point of view, the failed system must be unreliable. But from a safety point of view, the system is safe because it is designed conservatively so that the RPS automatically generates the channel trip signal for the failed channel. If any unrecognized failure happens in the RPS, then the RPS cannot shut down the reactor on demand. This case will not satisfy the reactor safety requirement, because the undetected failure may disturb the proper RPS operation. As a result, the quantitative safety is defined as the probability that the system operates correctly or fails in a safe manner.

Design Criteria

The following criteria is normally taken into account during the design of the Reactor Protection System in any research reactor:

- *Redundancy and diversification* - In order to achieve the requested system reliability and avoid common failures, these issues are basic design criteria.
- *Safety* - As for the RPS, the most important item is safety, which means the RPS must initiate the trip signal to shutdown the reactor whenever required. The measures to ensure safety are indicated by: safety software in high quality (safety class), defense-in-depth, selfcheck mechanism, error detection mechanism, and fail-safe principle.
- *Reliability* - In general, the reliability of the system should be < as 10° failure/demand. The reliability of the RPS must also be ensured, which means that RPS should work reliably as not to trip the reactor falsely. The measures to ensure reliability are characterized by: safety software in high quality, high precision and disturbance-resistance inhered in the digital processing, the filtering and pre-conditioning for the sampling data which can reduce the disturbance and random noise in sampling data and reduce the false-trip probability.
- *Availability* - In general, a modular design and use of redundant channels increase the availability of the system
- *Performance* - The response time of the system to any trip event is requested by international standards to be less than 60 ms. This time includes the sensing time, actuator to switch status.
- *Priority* - Signals from/to safety systems have higher priority of treatment than those signals from/to safety related and non safety systems.
- *Independence* - Physical and electrical isolation of the system enable its fully independence from other systems.

- *Single failure* - Sufficient redundancy and electrical independence shall assure that no single failure results in a loss of any protective function.
- *Fail safe* - The instrumentation of the system shall be designed so that any failure requests the initiation of the corresponding protective action. This criteria can be accomplished using dynamic signals (e.g. pulse train type signals) for normal conditions and static signals for trip conditions. Should an instrument or unit of the system fail, the pulse train disappears requesting trip (fail-safe principle).
- *Common failures* - In general, diversification of paths, physical and functional separation of equipments and channel redundancy are good practices to avoid common failures.
- *Automatic initiation* - All protective actions are automatically triggered by the reactor protection system without operator intervention. The operator may initiate protective actions manually; however, he cannot interrupt or interfere with any automatic action.
- *Manual initiation* - All protective actions are normally triggered automatically but they can also be triggered manually on operator's request. Nevertheless, once a protective action is initiated, manual actions cannot prevent or interrupt the normal execution of the required protective action.
- *Electrical isolation* - All signal paths from and to the instrumentation of the reactor protection system shall have decoupling devices in order to electrically isolate the system The protective functions of the system shall not be affected by a failure in an individual channel of the reactor protection system or in any other instrumentation of any safety related or non safety system.
- *Electrical power independence* – The uninterruptible power supply should be used to satisfy all power requirements of the system, to increase availability of the system, to reduce electrical noises, and to reduce the amount of spurious trips

The purpose of the RPS is to prevent the release of radioactive material to the environment. To meet this objective, the RPS may trip the reactor to prevent unsafe operation which could lead to accident conditions. Selected processes are measured by analog circuitry for trip set point comparison and then compared in digital logic circuitry to initiate action. Safety actions are based on the number of analog signals which have exceeded their respective set points.

DIGITAL REACTOR PROTECTION SYSTEM

As is well known, the conventional analog reactor protection systems (RPS) based on relays and other analog devices have many weaknesses, such as large number of components needing large equipments, many connection lines, drift of the setpoints, lack of online self-checking capability, lack of spare parts supply, etc. Therefore, the digital RPS which is based on computers and software will be widely accepted in the future due to its distinct advantages.

The advantages of a digital RPS are overwhelming, such as small size for the equipments, decrease in components, dramatic reduction of connection lines due to network techniques, stability and high precision for the setpoints, high tolerance for disturbances, low distortion in the process of information transferring and treatment, insensitivity to spurious signal and circuit deviation. The digital RPS is also characterized by the capability of implementing more complex and accurate algorithm, lower failure probability, online self-checking and self-diagnosis, and a friendly man–machine interface to show the state of the RPS transparently. In addition, the digital RPS should have the feasibility of modifying the logic during the design phase. With the challenge of licensing, the safety and reliability of the RPS should be guaranteed and proven by special designed architecture and through a strict verification and validation (V&V) program.

Digital systems have the following advantages over analog systems:

- Fewer characteristics change due to aging.
- Easier configurability as a redundant system.
- Easier modification and addition of new features by changing the system software.
- Improved maintainability by introducing self-diagnosis, self-calibration, event and data recording, and so on.

RPS ARCHITECTURE

There are four detection sensors namely fission chamber, ion chamber, gamma detector for the neutron flux and two temperature thermocouples of two fuel rods for the protection and safety of the reactor. All signals are connected by hardwire to two RPS (Reactor Protection System) for measurement and control. These two RPS channels are independent of each other. The output of the RPS is connected to the FAL (final actuation logic) on the decision made to protect the reactor. The FAL output will control the activation of the electromagnet either to release or holding the four control rods. The movement or the distance travel of the control rods will also be monitor by the CMS (Control and Monitoring System).

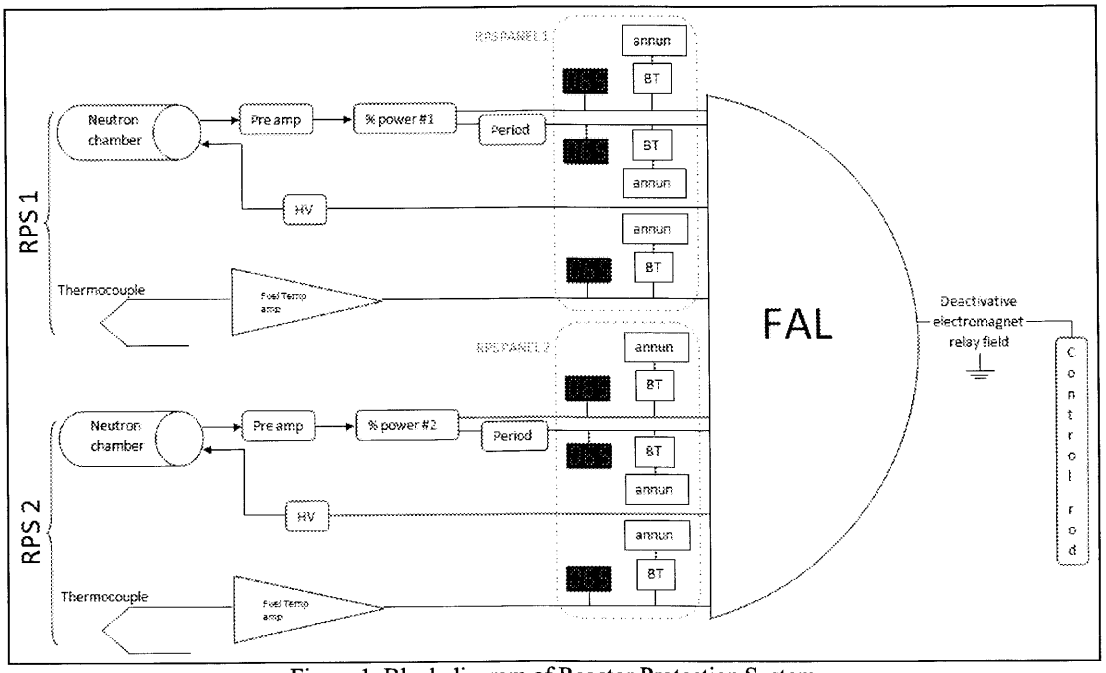

Figure 1. Block diagram of Reactor Protection System

The neutron chambers are located in the core in a fuel element position in a special water proofed container, which provides shielding, moisture proofing, and physical support for the detector and cabling. These chambers sense flux level changes and provide current signals to the various channels for monitoring. The Reactor Protection System 1 and 2 form a completely independent channel whereby there is no circuit or even the power supply is shared such that it forms a complete redundancy. This is shown in Figure 1. Any fault occurring in any of the channel will not affect the other channel. As shown in Figure 1, the two safety channels which are made of solid-state current amplifiers obtain their signals from two separate neutron chambers. Both channel amplifiers feed signal to percent-power meters and solid-state bi-stable trip protection circuits that drive the SCRAM logic. The two safety channels are mounted in separate drawers on either side of the console and are completely independent and redundant. Two high voltage (HV) supplies that bias the fission chambers are monitored by circuits that drive the SCRAM logic whenever HV failure occurs. A bi-stable trip circuit that drives the SCRAM logic compares the power signal level to a set level. Whenever it crosses the set level, a signal will de-energize a relay and cut the power supply to the rod carrier electromagnet and causes a POWER SCRAM. As shown in Figure 1, the fuel temperature channel receives its input from a chromel-alumel thermocouple embedded into two separate instrumented fuel element. The signal is amplified to drive a meter, recorder and SCRAM logic. For redundancy, two fuel temperature channels with meter readouts and SCRAM logic input are provided in both steady state and pulsing modes of reactor operation. The fuel temperature channels are mounted in the left- and right-hand drawers of the console.

During operation the RTP protection systems commence at Neutron or Power Measuring Channels and Fuel Temperature Measuring Channels. The neutron detector signals are fed into electronic circuitry that generate a period signal, rod withdrawal prohibit as well as percent power. A trip logic circuit that generates power SCRAM receives its signal from fission chamber high voltage monitor, fuel temperature, period, source level rod withdrawal prohibit and percent of output power.

All power channels include a means of CALIBRATING and TESTING the channel and a means of testing the protective trip level and power SCRAM. These calibrate and test circuits are built into the console as part of each channel. For redundancy, two fuel temperature channels with meter readouts and SCRAM logic input are provided in both steady state and pulsing modes of reactor operation. The fuel temperature channels are mounted in the left- and right-hand drawers of the console. The channels are provided with CALIBRATE and TRIP TEST switches located on the drawer front panels to allow verification of the fuel temperature readout and functioning of bi-stable trip that drives the SCRAM logic circuits. This allows failures to be detected before the reactor is brought into criticality.

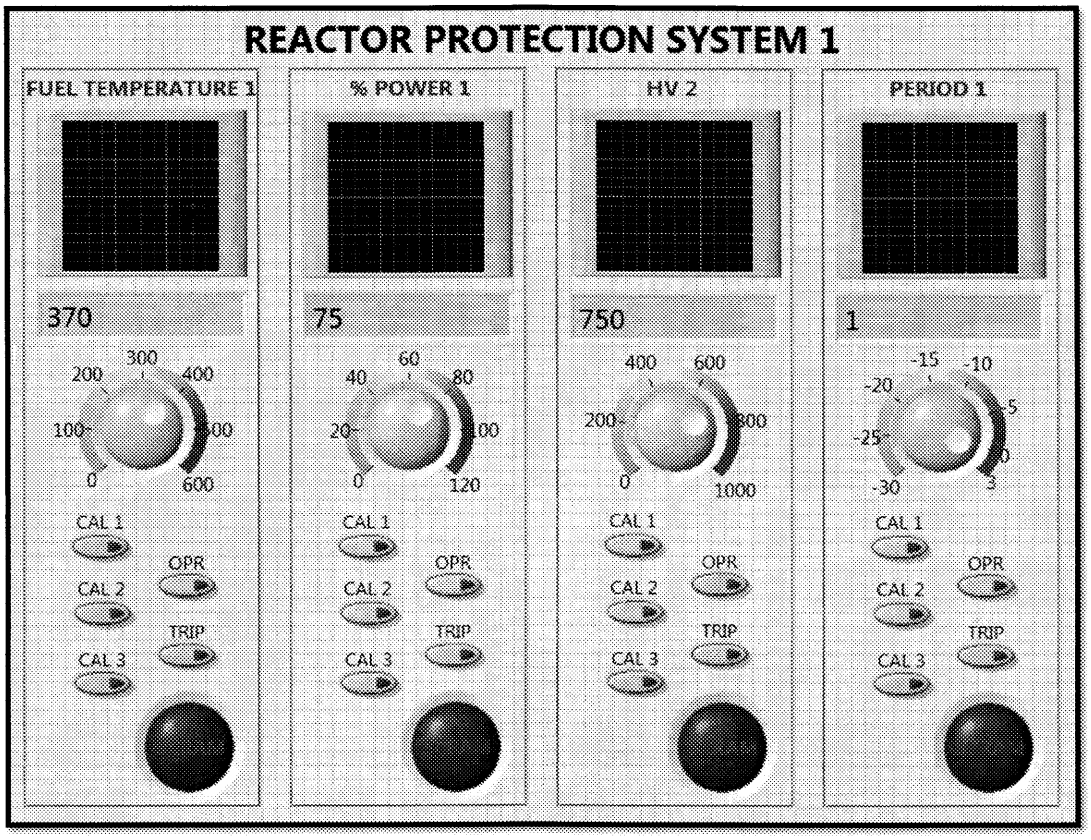

Figure 2. Digital RPS 1 Display

Figure 2. shows the proposed display of the Reactor Protection system 1. All stages in RPS are completely independent from one to another. The RPS has two redundancy channels. The number of analog channels has been changed to two with one out of two logics. This makes it possible to bypass a channel for testing and maintenance without losing redundancy and so improves the reliability of the system

SCRAM

A manual SCRAM button that disconnects the current of the control rod electromagnet is also provided for the operator; in case that the operator felt that immediate shut down is necessary.

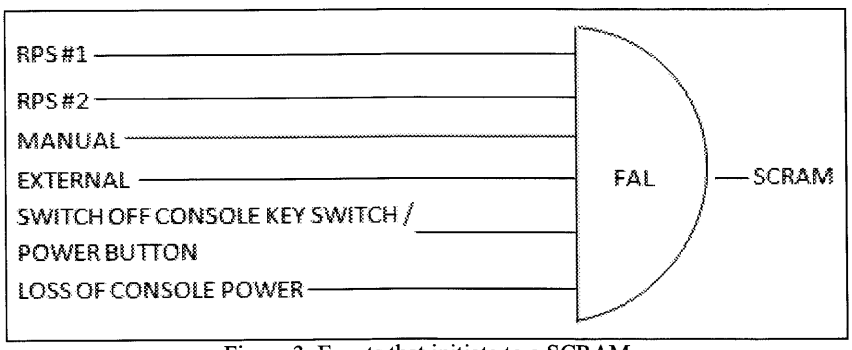

Figure 3. Events that initiate to a SCRAM

Referring to Figure 3., the following events will lead to the reactor power to SCRAM:
- Manual SCRAM button is pressed
- Loss of main supply to the I&C system console either by switching of the console key switch, power button or incoming supply not available
- Loss of high voltage for the neutron detectors
- Loss of +28-V supply for the control rod armature
- Percent Power exceed the trip set limit
- Fuel temperature exceed the trip set limit
- Opening the I&C console drawer top cover

Although all I&C circuits are energized at all times when power switch is ON, the rod drive electromagnet power can be obtained only through the key switch mounted on the front of the console. This will prevent unauthorized operation of the reactor and yet allow checkout and calibration of instrument channels by maintenance technicians.

Manual SCRAM

The control system is equipped with manual SCRAM switch on the console whereby the operator can press a bar and release all rods into the core. This is accomplished by disabling the voltage supply for the ectromagnetic carrier of the rod and the air valves of transient rod via the interlock circuit and SCRAM logic. The manual scram allows the operator to shut down the system if an unsafe or abnormal condition occurs.

External SCRAM

Apart from the above conditions, control rod release or SCRAM can also occur due to a trigger to the interlock protection circuit whenever the drawers on the left and right side of the console where all electronic circuits are placed are opened. This forms a protection against any tampering to the I&C systems.

The fuel temperature, power level, and period scrams provide protection to assure that the reactor can be shut down before the safety limit on the fuel element temperature will be exceeded. Table 1. shows the specifications to initiate a reactor scram for the primary purpose of protecting the reactor. This specification applies to the scram settings which prevent the safety limit from being reached.

Table 1. Setting and limitations to initiate SCRAM

	Parameter	Range	SCRAM condition
1	Fuel Temperature 1	0 – 600 °C	≥ 500 °C
2	Fuel Temperature 2	0 – 600 °C	≥ 500 °C
3	Percent Power 1	0 – 120 %	≥ 110 %
4	Percent Power 2	0 – 120 %	≥ 110 %
5	High Voltage 2 (for Percent Power 1)	0 – 1 000 V	≤ 75% of nominal

6	High Voltage 3 (for Percent Power 2)	0 – 1 000 V	≤ 75% of nominal
7	Period 1	-30 - +3 sec	≥ +3 sec
8	Period 2	-30 - +3 sec	≥ +3 sec
9	External (RPS 1 Cabinet Door)	NA	open
10	External (RPS 2 Cabinet Door)	NA	open

CONCLUSION

The RPS and the safety actuation system are designed to shut the reactor down, keep it shut down and ensure core and system cooling if plant parameters exceed plant safety limits. As a measure of defence in depth, safety limits for RPS actuation are set below calculated allowable limits to ensure that any unanticipated delays in protection system response will not cause unacceptable consequences. The introduction of digital systems in place of analog systems in some areas of the protection systems has simplified surveillance testing and reduced the duration of plant shutdown for testing.

It is obvious that digital safety protection systems can be applied to future research reactor. It is because safety protection systems using circuits composed of analog instruments and relays with relay contacts is difficult to realize from various reasons, such as securing their parts, cost, and preservation of manufacturing and maintenance personnel. And, an application of digital technology can be said a logical conclusion also in the light of its functional superiority. Therefore, it is necessary to make efforts to solve the issues in applying digital technology to safety protection systems. And, as there exist its actual performance, it is necessary to closely study the application processes, related standards and experiences.

The reactor I&C system is designed to detect any occurrence of abnormalities and protect the reactor from untoward incidents. The protection system is primarily made of a measurement system as described before and a logic circuitry that prevents the control rods from being withdrawn or forces the control rods to be inserted into the core instantly and SCRAM the reactor power. Power SCRAM is realized by disconnecting the supply of electric current to the electromagnet that carry and release the control rod armature.

REFERENCES

A Safety Assessment Methodology for a Digital Reactor Protection System: Dong-Young Lee, Jong-Gyun Choi, and Joon Lyou (2006), International Journal of Control, Automation, and Systems 105-112

Digital Instrumentation and Control Systems for Safety System and Main Control Room Design in Japan Nuclear Power Station (2007)

The first digital reactor protection system in China: Fu Li, Zijue Yang, Zhencai An, Liangju Zhang (2002) Nuclear Engineering and Design 215–225