Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 22, 2009

A Concept Design of Reactor Protection System for PALLAS Research Reactor

Young Rok Sim [a*], Sung Hun Kim [a], Jung Seon Kim [a], Geun Ok Park [b], In Soo Koo [b], Hee Seok Park [c], Gi Ho Cho [c]
[a] *Control Tech. Research Inst., SEC Ltd., 974-1 Goyeon-ri Woongchon-myon, Ulju-gun, Ulsan, Korea, 689-871*
[b] *Div. of I&C and HFE, KAERI, 150 Dukjin-dong, Yuseong-gu, Daejon, Korea, 305-353*
[c] *OPENCULTURE Co., Ltd., 395-12 Doryong-dong, Yuseong-gu, Daejon, Korea,305-340*
[*] *Corresponding author: syr1312@sanchang.com*

1. Introduction

The Reactor Protection System (RPS) is classified as a Safety Category 1 (SC1) I&C systems and complies with IEEE standards for Class 1E equipment. The RPS consists of First Reactor Protection System (FRPS) and Second Reactor Protection System (SRPS). There are two independent and diverse RPS to safely shutdown the reactor under all circumstances. The FRPS generates signals to actuate reactor trip by using CEA Bank1 automatically whenever monitored process variables reach predefined limits. The SRPS generates signals to actuate reactor trip by using Second Shutdown System (SSS) absorber assemblies automatically whenever monitored process variables reach predefined limits. The SRPS is an analogue system while the FRPS is a digital system. The RPS block diagram between the FRPS and the SRPS is given in Figure 1.

2. Methods and Results

2.1 Safety Concept

According to the regulations of nuclear law the main objectives of nuclear safety are [1, 2, 3, 4]:

1) The reactor must be safely shut down under all circumstances.
2) The decay heat must be safely removed in all situations.
3) No inadmissible release of radioactivity to the environment must occur.

2.2 System Description

During power operation, the FRPS is configured for 2 out of 3 trip coincidence with automatic initiation of protective functions requiring no operator action. The design includes provisions to convert the trip coincidence to 1 out of 2 during maintenance and testing. The FRPS Safety Soft-Controllers are provided to initiate operating bypasses and variable setpoint resets as necessary during reactor start-up and shutdown maneuvers. The FRPS has three channelized cabinets (see Figure 2).

The Bistable Module in each the FRPS channel receives process and discrete safety signals from the Process Instruments and Nuclear Instruments. The FRPS produces discrete output signals from each channel including:

- Pre-trip and Trip signals for each safety function, which are used for safety function status indication.
- Pre-trip and Trip signals used for reactor shutdown initiation, status and alarms.

The Bistable Module compares the process variable measurement to predefined limits. The bistable functions that cause unnecessary trips during reactor start-up and shutdown are provided with operating bypasses that block the trip function when it is unnecessary. The operating bypass is able to be manually entered by the operator in each channel, when the process is within a predefined range and is automatically removed when the process is outside the predefined range. The bistable function also generates a pre-trip signal which affected by the operating bypass in the same manner as the trip signal. The trip outputs from a channel's Bistable Module are distributed to Coincidence Modules in the same channel and to the redundant Coincidence Module in the other channels via safety communication network.

The Coincidence Module in a channel receives the trip outputs from the same channel and the Bistable Modules in the redundant channels. The Coincidence algorithm determines the state of the coincidence output based on the status of the three trip inputs and their respective trip channel bypass inputs. The trip channel bypasses are manually initiated in each channel from the Maintenance & Test Panel (MTP). The trip channel bypasses are permitted for channel maintenance and testing at power. The state of the coincidence output is tripped whenever at least two of the three trip inputs are present and none of the three trip channel bypasses are present. A trip channel bypass blocks its respective trip input in the Coincidence Module and change the coincidence logic to one out of the remaining two trip inputs. A reactor trip initiation signal is generated whenever a two out of three trip condition is sensed in the Coincidence Module for a particular function. The Coincidence Module outputs for reactor trip are sent to Reactor Trip Initiation Module for reactor trip. In order to send reactor shutdown signal to actuate four shutdown control elements, Reactor Trip Initiation Module (RIM) performs algorithm and generates Digital Output (DO).

Each trip channel bypass initiated from an MTP is sent to Coincidence Module in the MTP's respective channel. A Coincidence Module communicates with the other two redundant the FRPS channels to obtain the trip channel bypass status via safety communication network. The three trip channel bypass signals are processed by a verification algorithm in the Coincidence Module to ensure only one of the three channel bypass is active at a time.

The Coincidence Module initiates a bypass error indication if more than one trip bypass is attempted for the same trip parameter. Each trip channel bypass initiated from the MTP is also sent to Bistable Module in the respective channel. Each Bistable Module sends all its trip channel bypass status to the MTP in the other two channels via the safety communication network. The MTP initiated trip channel bypasses and annunciate discrepancies.

Within each channel the Bistable Module, Coincidence Module, Reactor Trip Initiation Module, the MTP communicate with each other using safety communication network. The FRPS is designed for fail-safe operation under component failure or loss of electrical power. A channel reactor trip initiation is initiated whenever an applicable component fails. The system is capable of satisfactorily performing its intended function for a surveillance period without recalibration throughout the range of worst case environmental and power source conditions excluding seismic events.

The SRPS generates signals to actuate element-type neutron absorbers automatically. It provides status outputs for operator monitoring for reactor shutdown system. The SRPS has three channelized cabinets which are located in the Equipment Room. Trip signal automatically generated from the SRPS overrides signal automatically generated from the FRPS.

2.3 Failure Modes and Effect Analysis

The Failure Modes and Effect Analysis, commonly referred to a FMEA, is one of the most utilized methods for conducting reliability analyses. The Failure Modes and Effects Criticality Analysis (FMECA) is really an extension of the FMEA, focusing on the quantitative parameters for a criticality assigned to each probable failure mode, and is discussed below. A widely accepted military standard for conducting FMEAs is the MIL-Std-1629. This military standard details the specifics in conducting a FMEA. The result of the FMECA is based on the RPS safety signals.

The criticality (risk priority) is defined as S (Severity) $\times$ O (Occurrence) $\times$ D (Detection).

Whenever a design or a process changes and detailed design progresses, an FMEA will be updated. The result of FMEA is given in Table 1 and Table 2.

1) Level A - Frequent. The high probability is defined as a relative probability which is high of the overall system probability of failure during the defined mission period.
2) Level B - Reasonable probable. The reasonable probability is defined as relative probability which is medium of the overall system probability of failure during the defined mission period.
3) Level C - Occasional probability. The occasional probability is defined as a relative probability, which is low of the overall system probability of failure during the defined mission period.

3. Conclusions

The RPS consists of two functionally independent and diverse protection systems that initiate, among other actions, automatic reactor shutdown. The protection and monitoring functions of the RPS have been designed to ensure safe operation of the reactor. The RPS is aimed at avoiding fuel damage and preventing the release of radioactive material from the reactor pool. These actions can be accomplished either automatically or manually.

For the future, use of digital I&C systems for safety applications will be the usual practice. Possibilities to take advantage of advanced analytical methods will still increase opportunities for optimization of safety standards and plant operation in future.

REFERENCES

[1] IAEA NS-R-4, "Safety of Research Reactors", 2005
[2] IAEA 50-SG-D1, "Safety functions and component classification for BWR, PWR and PTR", 1979
[3] IAEA 50-SG-D3, "Protection System and related features in nuclear power plants", 1980
[4] IAEA NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants", 2002

Table 1. FRPS FMEA

FRPS	Criticality		
	Startup	P-Operation	Grade
PCS Pressure	C	C	C
Reactor Inlet Temperature	C	C	C
Core Temperature Difference	C	C	C
Reactor Outlet Temperature	C	C	C
PCS Flow	C	C	C
Reactor Radiation (Delayed Neutron) for Fuel Failure	B	B	B
Pool Surface Radiation	A	A	A
Pool Water Level (Lo)	B	B	B
Neutron Logarithmic Power	C	B	C
Neutron Linear Power (Hi)	C	B	C
Neutron Logarithmic Power Rate (Hi)	C	A	B
Neutron Detector Low Voltage	C	C	C
Seismic Level	C	C	C

Table 2. SRPS FMEA

SRPS	Criticality		
	Startup	P-Operation	Grade
Gamma Power Meter (N-16)	B	B	B
Pool Water Level (Lo-Lo)	B	B	B
Neutron Linear Power (Hi-Hi)	C	B	C
Neutron Logarithmic Power Rate (Hi-Hi)	C	A	B
FRPS Trip	A	A	A

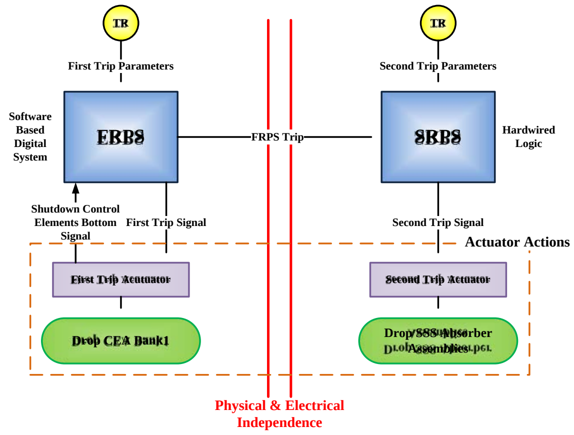

Figure 1. RPS Functional Block Diagram

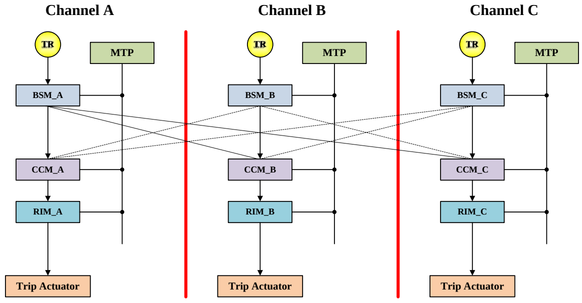

Figure 2. FRPS Functional Block Diagram