A Reliability Study for RPS in Jordan Research & Training Reactor

EL-Bordany Ayman [a], Won Young Yun[b*]
[a] Nuclear and Quantum Engineering Department, Korea Advanced Institute of Science and Technology (KAIST), 373-1 Guseong-dong, Yuseong-gu, Daejeon 305-701
[b]Korea Institute of Nuclear Safety(KINS),62 Gwahak-ro, Yuseong-gu, Daejeon 305-338
[*]*Corresponding author: k034ywy@kins.re.kr*

1. Introduction

Plant protection system (PPS) of Jordan Research Reactor consists of Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). The RPS provides an emergency shutdown of the reactor to protect the core and the reactor coolant system pressure boundary. The ESFAS provides those functions required to prevent the release of radioactive material to the environment in the event of pressure boundary rupture. In general, the RPS goes down the line 2-out-of-m redundant channel to emphasize a reliable operation.

This paper presents the reliability assessments accordant with the RPS unavailability of Jordan Research and Training Reactor (JRTR). In order to figure out the RPS unavailability of JRTR, the Advanced Information Management System (AIMS) code developed by Korea Atomic Energy Research Institute (KAERI) was applied. AIMS code is a PSA model for building event tree, fault tree, calculate the cut-sets of the fault tree, and also generate common cause failure (CCF) using alpha factor model, and so on. Accordingly, the unavailability of the RPS was calculated using AIMS code for assuring safety of the JRTR.

The JRTR RPS provides the protective action to shutdown the reactor and also provides Engineered Safety Features (ESF) actuation function to mitigate the consequence of accidents. RPS is a class 1E instrumentation and control (I&C) system which mitigates the Anticipated Operational Occurrence (AOO) and accidents. The RPS of JRTR is designed with a digitalized safety system that causes a reactor trip to protect the core by generating trip signal to insert four Control Absorber Rods (CARs) and two hydraulic actuated Second Shutdown Rods (SSRs) into the core whenever the trip parameters exceed the trip set-points. In addition, the RPS provides engineered safety features actuation signal to mitigate the consequences of accidents and to prevent the release of radioactive material to the environment. The RPS of JRTR consists of three redundant channels and each channel consists of sensors, bistable processor (BP), coincidence circuit (CC), initiating circuit (IC), actuation circuits (AC), interface and test processor (ITP), maintenance and test panel (MTP), and other equipment necessary to monitor selected reactor conditions and to provide the reliable and rapid reactor protective action. Each channel has independent measurement with electrical isolation and physical separation is provided for each parameter used for the direct protective action of the RPS.

The basic block diagram of the JRTR RPS is shown in Fig 1. This diagram shows the communication interface among the cabinet which consists of three channels. Channel A, B, and C are identical in content and each channel contains a subset of the equipment to provide a three channel redundancy. Each channel has its own measurements (independent measurements), with electrical isolation and physical separation.

There are twenty two trip parameters monitored by bistable processors. There are three bistable processors per channel, and the BP consists of Tricon Programmable Logic Controller (PLC), which has triple redundant architecture and bistable processor performs 2-out-of-3 voting logic in order to provide the high integrity and there is no single failure in case of the uninterrupted process operation. Nuclear sensors send the signals into the analogue input module of the bistable processor, and there are three processor modules in the BP scan the analogue input module and convert the process signals to engineering values. The three processor modules compare engineering values with those of the set-points and send the results to the digital output module (DOM). After that, DOM send a contact signal through hardwire to the CC of the same and different channels. Each BP has two digital output signals, those signals provided to the CC, which prevent a single failure of the digital output to affect the safety function.

There are three coincidence circuits (CCs) for each channel same as BP and are located in one cabinet. One of the CCs is for reactor trip, and the rest two are one for the Siphon Break Valve (SBV) and the other Confinement Isolation Damper (CID) actuation; respectively. Each CC consists of six relays which are arranged with 2-out-of-3 logic in order to deactivate the power from Control Rod Drive Mechanism (CRDM)/ Secondary Shutdown Drive Mechanism (SSDM) or SBV or CID. CRDM, SSDM, SBV, and CID initiation circuit receive the actuation signal from the CC which are made of the under voltage trip relay circuits. There are six initiating circuits (ICs) such as CRDM, SSDM, SBV, and CID ICs which are located in one channel. ICs generate the automatic/manual reactor trip signals or ESF trip signals. Those signals from the ICs are combined with “Or logic” in the ICs, but physically it is connected with “And Gate” when the fault tree is

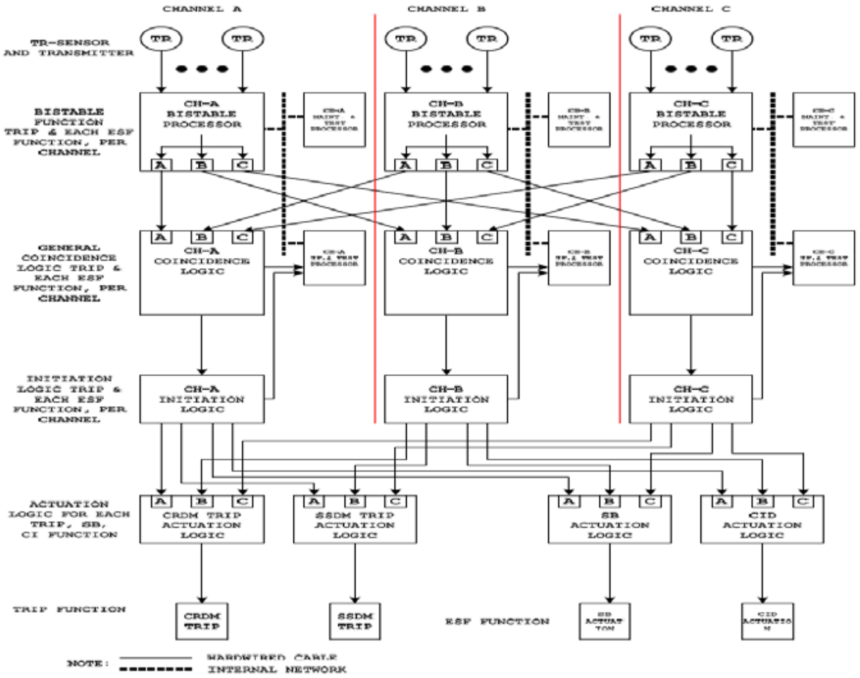

Fig. 1. JRTR RPS basic block diagram

constructed. It is because the current in the line can be transmitted to the trip actuation logic only when all the relays in series have failed. In other words, if at least one relay is alive among the relays in series, the current can be disconnected by that relay [1].

2. Research Scope

The major concern of this study is an unavailability calculation of the JRTR RPS. If the RPS of the JRTR does not generate the reactor trip signal on demand, the reactor will be in an unsafe state. In the meantime, the reactor will be in a safe state condition and can make safely shutdown when the RPS is operating well. In that case the reactor satisfies the safety requirements. If there is a failure in the RPS and the system detects that failure, automatic trip signal will be generated by the RPS and that will satisfy the fail-safe requirements of the RPS [2]. In case of automatically generating signal fails to trip the RPS, manual shutdown signal should be initiated by the operator. From the safety point of view, a failed system is reliable and the system will be safe because it is designed conservatively. However, from the reliability point of view, the system is unreliable. So, if there is a failure in the channel, the RPS generates an automatic trip. In case of an undetected failure in the channel, the RPS cannot shutdown the reactor on demand; in that case the reactor safety will not be satisfied because the RPS operation may be disturbed by the undetected failure [2].

Fault tree analysis (FTA) model describes the failure events probabilities of the JRTR RPS and calculates the unavailability of the system by making summations for all cut-set events. The failure events of the JRTR RPS represent in the random failure of the hardware components, common cause failure (CCF), operator errors, and so on.

2.1 Description of the Basic assumption

In order to calculate the unavailability of the JRTR RPS, the failure data must be available from the manufacturer or the assumption data can be considered. In this paper, the proposed data were considered and taken from Hanul nuclear power plants (NPP) units 5&6 [3], and also from NUREG/CR-5500, Vol.10 [4], due to the shortage of the given data. Table 1 shows the chosen failure data from Hanul NPP unit 5&6 and NUREG/CR-5500, Vol.10. The first column in the given table below consists of the hardware failure events of the reactor protection systems and the operator failure. The second and the third columns in Table 1 below describe the failure rates of the hardware components of the RPS and the failure rate of the operator.

Table 1: Failure rates of the RPS

Module	Failure rates 1	Failure rate 2
Processor module	1.17E-03	5 E-04
Analog input module	7.2E-04	7.6 E-03
Digital output module	2.95 E-04	2.7 E-03
Relay Failure	6.2 E-06	1.2 E-04
Logic Relay Failure	--	2.6 E-04
Operator Failure	5 E-02	1 E-02
Switch Failure	1.5 E-05	1.3 E-04
Sensors failure	4.5 E-03	1.1 E-04

Failure rates 1: Chosen failure data from Hanul NPP unit 5&6.
Failure rate 2: Chosen failure data from NUREG/CR-5500, Vol.10.

2.2 Fault Tree Analysis Model

The basic event of the fault tree of the RPS consists of hardware failures, operator failure or manual trip failure. The FTA for the RPS consists of automatic trip and manual trip signals. The process parameter input signals for the reactor trip function are compared to pre-determined fixed trip set-point values in the bistable processors (BPs). If any two measurements of a given process parameter exceeded the set-point value, the coincidence signals are generated by a two-out-of-three coincidence circuit. The affected coincidence signals are latched in initiation circuits. The actuation circuits receive initiation trip signals from ICs and actuate CARs and SSRs using two-out-of-three voting mechanism in its own circuits. The RPS automatically initiates reactor shutdown by inserting four CARs and two hydraulic-actuated SSRs into the reactor core. The CARs are dropped down freely by disconnecting the electricity to the electro-magnet. The SSRs are inserted by cutting off the power to the solenoid operated piston valve installed in the piping of the hydraulic pump. The RPS is designed to fail-safe, by means to shut down the reactor when it is de-energized due to the loss of electrical power supply [1].

In this paper, we consider only the failure of the CRDM actuation circuit because the SBV and CID have the same circuits and it will give the same output results. The applied assumption for making fault tree is to compare the fault tree with and without manual trip. The failure of the manual trip is due to the failure of the switch itself or the operator fail to trip the RPS. Human actions can affect the unavailability of the RPS. The data taken from Hanul nuclear power plants (NPP) units 5&6, and also those from NUREG/CR-5500 is used to calculate the unavailability of the RPS. The unavailability of the RPS is calculated by making summation of all cut-sets.

2.3 Common Cause Failure Model

The occurrence of CCF in the RPS prevents the RPS to take appropriate safety action in case of the plant conditions approaching to certain safety limits. Thus, a CCF of the RPS has a rigorous impact on the safety analysis of research reactor.

The failure criteria of the CCF must meet all of the following criteria: (1) the failure of the individual component for two or more components, that failure may be from in-service testing, failure during demand, or failure because of degraded components; (2) the failure of components within a specified period of time; (3) the failure of the components from single shared cause and coupling mechanism; and (4) Failure of a component occurs within the established component boundary [5].

There are several techniques for modeling the CCF probabilities such as Alpha factor, Beta-factor, and Multiple Greek Letters methods, etc. In this paper, the Alpha factor model is selected. Reasons for this choice are that the alpha factor model, **1)** is a multi-parameter model which can handle any redundancy level, **2)** is based on ratios of failure rates, which makes the assessment of its parameters easier when no statistical data are available, and **3)** has a simpler statistical model, and produces more accurate point estimates as well as uncertainty distributions compared to other parametric models which have the above two properties [5].

In this study, AIMS code generates the common cause failure probability of the RPS using Alpha Factor model including independent event. Table 2 shows the estimated CCF probabilities of the JRTR RPS obtained from AIMS code.

Table 2: Common cause failure probability of the RPS

Description	Prob.
Independent Event	3.8E-03
CCF (2/3)	4.26E-05
CCF (3/3)	4.04E-05
CCF (2/2)	8.52 E-05

The CCF generated data from AIMS code is used in the fault tree with the same assumption of the failure rates of the remaining events. In that case, the FT with and without a manual scram was built in order to understand what will happen if the operator interacts with the RPS after the automatic trip fails.

3. Results

In this study, the output results show the difference among the FTA models in many cases. In the first case, the FTA is compared with and without a manual trip. In the second case, CCF included in the fault tree and also compared with and without a manual trip. Fig.2 shows a fault tree of the JRTR RPS with automatic and manual trip signals. The top event of the JRTR RPS FTA model is the ‘RPSFAIL’. The event ‘RPSFAIL’ occurred when CARs fail to drop. The event ‘CRDMFAIL’ happens when ‘Failure of CAR1 or CBR1’ and ‘Failure of CBR2 or CCR1’ and ‘Failure of CAR2 or CCR2’ is happening. The event ‘CAR1CBR1’ happens when ‘Failure of CAR1’ or ‘Failure of CBR1’ is happening. The event ‘CAR1’ happens when ‘there is no signal to CARs or ‘the failure of the CARs itself’. The event ‘FCAR’ happens when the ‘Automatic Trip Failure for CH.A’ and ‘Manual Trip Failure for CH.A’ is occurring. The event ‘MANUALCHA’ happens when ‘Operator fails to initiate Manual Scram’ or ‘Manual trip switch in CH.A Fails’ is happening. This FTA model is determined from

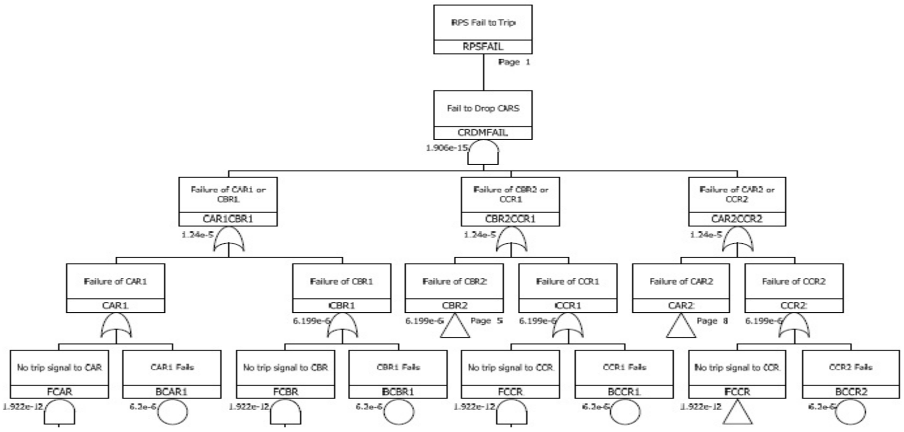

Fig. 2. A part of Fault tree model for JRTR RPS

the RPS architecture of Fig.1. This FTA modeling is so huge work that it cannot be presented in this paper. Fig.2 shows a brief example of the FTA for the RPS. The FTA model of Fig. 2 will be continued until it reaches to the basic event such as component failure probabilities, the common cause event, or human error [2]. Table 3 shows the unavailability results of the RPS. The safety assessment of the RPS is determined by summing up the individual probabilities of the basic events in the FTA model.

Table 3: Unavailability results of the RPS

Items	Unavil.1	Unavil.1 without manual scram	Unavil.2	Unavil.2 without manual scram
FT without CCF	4.569e-6	9.122e-5	3.252e-6	3.252e-4
FT with CCF	2.310e-4	6.004e-4	2.116e-4	9.470e-4

Unavil.1: Unavailability output after using data from Hanul NPP unit 5&6. Unavil.2: Unavailability output after using data from NUREG/CR-5500, Vol.10.

For the selected trip parameters such as pressure transmitter, differential pressure transmitter, level transmitter, and neutron flux detector, the safety assessment result of the RPS is shown in Table 4. These trip parameters are taken from a reliability study [7].

Table 4: RPS output result for specific parameters.

Trip Parameter	Failure Rate	Output 1	Output 2
pressure transmitter	7.99E-05/h	3.343E-06	2.116E-04
differential pressure transmitter	7.99E-05/h		
level transmitter	7.99E-05/h		
neutron flux detector	1.53E-05/h		

Output 1: Output result of the FTA using NUREG/CR-5500, Vol.10 with changing the sensor data only using the reference data from a reliability study.
Output 2: By using CCF.

4. Conclusions

The cut-sets are the various combinations of component failures or operator errors that result in the defined top event of the model. The intent of this evaluation is to determine the unavailability of the JRTR RPS by considering there is a shortage of the given data. So, calculated results of the JRTR RPS are summarized in terms of the probability that RPS would fail to trip the reactor on demand in Table 3.

It was found that the unavailability of the JRTR RPS reduced when the automatic and manual failure are combined together in one FT. And also, it was found that the data selected from the NUREG/CR-5500, Vol.10 is much better than the selected data from Hanul NPP unit 5&6. When the CCF added to the system, it will have a great effect on the system and the unavailability of the RPS will increase as shown in the Table 5. Finally, when the operator making a decision to trip the RPS in the case of the automatic trip failure, it will reduce the RPS unavailability as shown in the following Table 5:

Table 5: Reduced unavailability of the RPS

Items	Unavail.1 reduced by approximately%,	Unavail.2 reduced by approximately%,
FT without CCF	95% when manual trip added	99% when manual trip added
FT with CCF	61.5%	77.65%

Acknowledgements

The author's wishes to thank Prof. H. G. Kang from KAIST and Dr. S. K. Shin from KAERI for providing AIMS code and the information related to the RPS design of JRTR, respectively.

REFERENCES

[1] JR-681-KJ-414-001, Rev. 1, System Description for Reactor Protection System.
[2] Dong-young Lee, Joung-Gyun Choi, and Joon Lyou, A safety Assessment Methodology for a Digital Reactor Protection System, International Journal of control, Automation, and Systems, Vol. 4, no.1,pp.105-112,February 2006.
[3] ST-99-231, Rev.01, Unavailability Analysis for the Digital Plant Protection System, 1999.
[4] NUREG/CR-5500, Vol.10, November 2001, “Reliability Study: Combustion Engineering Reactor Protection System, 1984–1998”.
[5] NUEG/CR-5485, Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.
[6] KAERI-ISA-MEMO-AIMS-03-KOR, Reference manual of AIMS code.
[7] KAREI/TR-2164/2002, “Reliability Study: KSNP Reactor Protection System”.