Unavailability of RPS and ESFAS for the OPR-1000 Reactor

Seung-Cheol Jang*, Yoon-Hwan Lee, Seung-Jun Lee
Korea Atomic Energy Research Institute, 150, Dukjin-dong, Yuseong-gu, Daejeon, 305-353
**Corresponding author: scjang@kaeri.re.kr*

1. Introduction

The safety-related plant protection system (PPS) of the OPR-1000 reactor maintains plant safety by continuously monitoring selected plant parameters, and initiating appropriate protective action if any parameter reaches a limiting safety system setting. It consists of the reactor protection system (RPS) and the engineered safety features actuation system (ESFAS). The RPS designed for accident prevention provides an automatic or manual rapid shutdown of the reactor to protect the core and the reactor coolant system boundary. The ESFAS provides functions required to limit plant/equipment damage and to mitigate the consequences of the accident. It is designed for accident response and mitigation. This paper focuses the unavailability analysis of the RPS and was performed, based on the domestic operating experience of the OPR-1000 reactors.

2. Methods and Results

2.1 System Overview

The PPS comprising four identical protective channels can be roughly divided into three segments - bistables, logic matrices, and initiation circuits - as illustrated in Fig. 1.

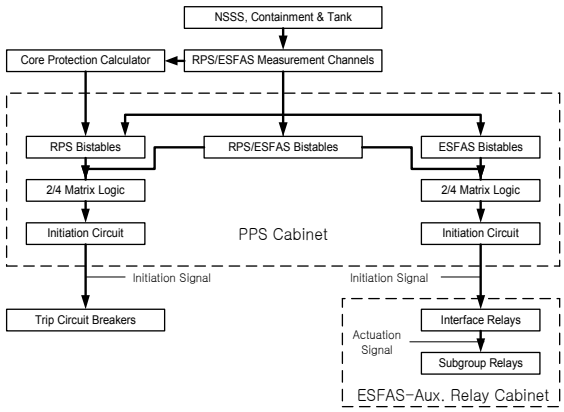

Figure 1. Simplified Block Diagram of the PPS in the OPR-1000 Reactor

Each protective channel has 15 and 10 instrumentation loops for the RPS and ESFAS, respectively. If an RPS trip is involved, the output of PPS will initiate a reactor trip via the trip circuit breakers (TCB). If an ESFAS trip is involved, the PPS will generate the appropriate ESFAS signal via auxiliary relay cabinets (ARC). Also, the OPR-1000 reactor has an alternate reactor trip system to mitigate anticipated transients without scram (ATWS), termed diverse protection system (DPS). The DPS comprising two protective channels is non-safety related system to provide trip signal for high pressurizer pressure, and actuation signal for the AFAS, independently.

As shown in Table 1, many different types of trip parameters are associated with the PPS. Except for the manual trip, the PPS includes 11 types of automatic trip parameters for the RPS and 6 types of functions for the ESFAS. Note that two digital signals related to thermal margin, e.g., local power density (LPD) and departure from nucleate boiling ratio (DNBR), are generated externally by core protective calculator (CPC), and input to each RPS channel.

Table 1. Plant Protection System Parameters

Trip Parameters	Abbreviation	RPS	ESFAS	ESFAS Function*
Variable Over-Power Trip	VOPT	X		
High Logarithmic Power	Hi LOG PWR	X		
High Local Power Density	Hi LPD	X		
Low DNBR	Lo DNBR	X		
High Pressurizer Pressure	Hi PZR PR	X		
Low Pressurizer Pressure	Lo PZR PR	X	X	SIAS, CIAS
Low SG-1 (-2) Level	Lo SG-1 (-2) LVL	X	X	AFAS
High SG-1 (-2) Level	Hi SG-1 (-2) LVL	X	X	MSIS
Low SG-1 (-2) Pressure	Lo SG-1 (-2) PR	X	X	MSIS
High Containment Pressure	Hi CTMT PR	X	X	SIAS, CIAS MSIS
Low SG-1 (-2) Coolant Flow	Lo SG-1 (-2) FL	X		
High-High Containment Pressure	Hi-Hi CTMT PR		X	CSAS
Low Refueling Water Tank Level	Lo RWT LVL		X	RAS

*) SIAS (safety injection actuation signal), CIAS (containment isolation act. sig.), MSIS (main steam isolation sig.), AFAS (auxiliary feedwater act. sig.), CSAS (containment spray act. sig.), RAS (recirculation act. sig.)

Before the changes of surveillance test intervals [1], the OPR-1000 analog-type RPS and ESFAS channels - bistables, logic matrices, initiation circuits - are tested on a sequential monthly basis. Generally, the channels to be tested are placed in bypass. Each train of the ESFAS ARC is tested every two months (on a staggered monthly basis). All of sensors/transmitters are tested and calibrated every refueling, except for refueling water tank levels tested every three months. DPS is tested every three months. Finally, each trip circuit breaker is tested seven times per month during operation, and five times during refueling.

2.2 System Modeling

The RPS or ESFAS failure is defined at the signal level, representing the failure of the RPS trip signal to trip the reactor on demand by interrupting power to the control element drive mechanism (CEDM) buses and

the failure of the ESFAS signal to actuate the required ESF components, respectively. Without loss of generality, the top events in the RPS/ESFAS fault trees can be described by "Failure of trip on demand." Modeled separately were 11-type automatic reactor trip signals and 6-type ESF actuation signals as listed in Table 1. The DPS model was also included in fault trees for high pressurizer pressure and the AFAS.

The RPS/ESFAS fault tree was developed based on as-operated design of the OPR-1000 reactor. The level of detail in the RPS/ESFAS fault trees includes measurement devices, CPC, bistables, bistable output relays, logic matrix relays, interposing relays, initiation relays, TCB with shunt and under-voltage trip devices, interface and subgroup relays in the ARC, signal processors and control circuits for the DPS, manual switches, and supporting system (*e.g.,* electric power).

Generally, four types of data are required for the quantification of the system fault tree, namely 1) independent component failure data, 2) common cause failure (CCF), 3) unavailability due to test and maintenance, and 4) human error probability.

The plant-specific component reliability data analysis was carried out for the system analysis ([1],[2] and [3]).

To obtain more realistic model for the post-accident operator error events, in particular, the manual reactor trip was divided into two conditions; 1) no reactor trip due to mechanical failures of all TCBs, and 2) no automatic trip signal. The failure probability for the first case was estimated to be 0.032, based on the results of simulator experiments. For the second situation, however, it was assumed to be 0.07 considering manual reactor trip by non-safety information in MCR and the functional dependency factor among the safety-related signals. According to the ESF actuation signals, the failure probabilities of manual actuation were estimated from 0.001 to 0.004 approximately, using the methodology of the NUREG/CR-1278 [4]. For the pre-accident event such as calibration error, it was conservatively assumed that there was high dependency between miscalibration events for an input parameter.

2.3 The Results and Insights

The system fault trees were quantified using the AIMS-PSA code [5]. The fault tree analysis results for the RPS and ESFAS are presented as probabilities that the RPS and ESFAS fail to perform their intended functions on demand, *i.e.*, unavailabilities.

The mean unavailability for each RPS trip parameter ranges from approximately 2.5e-5 to 2.0e-4, as shown in Table 3. The unavailabilities for digital trip signals (DNBR and LPD) and linear and log power signals (VOPT, LOG PWR) are comparatively higher than others, because of higher component failure probability for ex-core neutron flux measurement channels. The dominant contributors to unavailability of an RPS parameter are CCFs for elements within the trip channels coupled with failure of manual trip by operator, e.g., miscalibration, measurement loop, bistables, initiation relay, TCB, in order. Note that CCFs for initiation relay and TCB combined with failure of manual trip are more important contributors to the high-level risk measures, e.g., the frequency of anticipated transients without scram (ATWS), core damage frequency (CDF), etc. The uncertainty results for the RPS parameters are also involved in Table 3.

Table 3. Results of the RPS Unavailability Analyses*

Trip Parameters	Point Estimate	Uncertainty**			Remarks
		5%	50%	95%	
VOPT	8.02e-5	1.54e-5	5.38e-5	2.24e-4	
Hi LOG PWR	1.35e-4	2.51e-5	8.97e-5	3.71e-4	
Hi LPD	2.03e-4	4.11e-5	1.45e-4	5.43e-4	
Lo DNBR	2.03e-4	4.11e-5	1.45e-4	5.43e-4	
Hi PZR PR	2.58e-5	1.87e-6	1.12e-5	8.81e-5	w/o DPS
Lo PZR PR	5.09e-5	5.49e-6	2.73e-5	1.68e-4	
Lo SG LVL	2.54e-5	1.86e-6	1.11e-5	8.82e-5	
Hi SG LVL	2.54e-5	1.80e-6	1.11e-5	8.91e-5	
Lo SG PR	2.58e-5	1.99e-6	1.14e-5	8.67e-5	
Hi CTMT PR	2.58e-5	1.99e-6	1.14e-5	8.93e-5	
Lo RCS FL	2.53e-5	1.94e-6	1.14e-5	9.14e-5	

*) All Channels are in service. **) Monte Carlo sampling with the sample size of 10,000.

The resultant ESFAS mean failure probabilities with results of the uncertainty analysis are summarized in Table 4. Except for the AFAS, the ESFAS failure probabilities for signals are estimated to be approximately 4.53e-6 through 5.80e-6, which are proportional to the number of the corresponding input parameters (Refer to the Table 1). Note that the unavailability of 3.71e-8 for AFAS is due to credit for the DPS. The primary dominant cut set for the ESFAS signals involve common cause failure of interface relay/contacts in ARC. It is caused by no credit for a recovery action to actuate signal manually in ARC. Except for the CCF of interface relay/contacts, the overall dominant cut sets were CCFs of I&C components coupled with failure of manual actuation by operator on the main control panel.

Table 4. Results of the ESFAS Unavailability Analyses*

ESFAS Signals	Point Estimate	Uncertainty**			Remarks
		5%	50%	95%	
SIAS	4.81e-6	2.17e-7	1.72e-6	1.78e-5	
CIAS	4.81e-6	2.34e-7	1.73e-6	1.77e-5	
CSAS	4.53e-6	1.32e-7	1.45e-6	1.72e-5	
RAS	4.54e-6	1.50e-7	1.44e-6	1.72e-5	
MSIS	5.80e-6	3.69e-7	2.50e-6	2.08e-5	
AFAS	3.71e-8	1.04e-9	1.12e-8	1.43e-7	w/ DPS

*) All Channels are in service. **) Monte Carlo sampling with the sample size of 10,000.

3. Conclusions

This study was performed to provide useful insights for risk-informed applications like improvement of technical specifications for the OPR-1000 analog-type RPS and ESFAS. The following are some insights obtained from this study.

1) The mean unavailability ranges from approximately 2.5e-5 to 2.0e-4 for each RPS trip

parameter, and 3.7e-8 to 5.8e-6 for each ESFAS signal.

2) To obtain more realistic model for the post-accident operator error events, the manual reactor trip was divided into two conditions; no reactor trip due to mechanical failures of all TCBs, and no automatic trip signal. The cautious attention has to be paid for the modeling and estimation of human error events because it causes very sensitive changes in priorities of minimal cutsets.
3) The dominant cutset for the ESFAS signal is CCF of interface relay/contacts in ARC. It can be improved by an additional procedure of operator manual actions recoverable in ARC.

ACKNOWLEDGEMENTS

This work was supported by Nuclear Research & Development Program of the National Research Foundation of Korea (NRF) grant, funded by the Korean government, Ministry of Science, ICT & Future Planning. Also, the authors would like to acknowledge the cooperation of the Korea Hydro and Nuclear Power Co. (KHNP) for data collection.

REFERENCES

[1] S. C. Jang, *et. al.*, 2012, Improvement of Risk-Informed Surveillance Test Interval for the Safety-related I&C System of Ulchin 3&4, KAERI/TR-4558/2012, Korea Atomic Energy Research Institute.
[2] S. C. Jang, *et. al.*, "Reliability Data Analysis of the KSNP Safety-related I&C Components from Operational Experience Data during the Period of 2003 through 2007", Transactions of the Korean Nuclear Society Spring Meeting, Gwangju, Korea, May 30-31, 2013.
[3] S. C. Jang, "A Case Study of the Plant-specific CCF Parameter Estimation for the Safety-related I&C Components Using Bayesian Update Technique", Transactions of the Korean Nuclear Society Spring Meeting, Gwangju, Korea, May 30-31, 2013.
[4] Swain, A. D., and Guttmann,H. E., 1983, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission.
[5] S. H. Han, and S. C. Jang, "AISM-PSA: A Software for Integrating Various Types for PSAs, PSAM-9 Conference, Hongkong, May 2008.