Transactions of the Korean Nuclear Society Autumn Meeting
Busan, Korea, October 27-28, 2005

Fault Tree Analysis of the ESFAS Actuation Signals for KSNP

Seung-Cheol Jang, Kyung-Ran Min, Seok-Joong Han
Korea Atomic Energy Research Institute,150, Dukjin-dong, Yuseong-gu, Daejeon, 305-353
scjang@kaeri.re.kr

1. Introduction

The performance and unavailability analysis of the engineered safety features actuation system (ESFAS) was performed, based on the operating experience of the Korean standard nuclear power plant (KSNP). The ESFAS unavailability was evaluated by the system fault tree analysis (FTA), based on as-built/as-operated design and the plant-specific component reliability data. The sensitivity analysis was also performed according to some configuration changes decribed as limiting conditions of operation (LCO) in technical specification.

2. Overview of the ESFAS

The ESFAS provides ESF acuation signals required to limit plant/equipment damage and to mitigate the consequences of the accident. There are 6-type ESF actuation signals, e.g., SIAS (safety injection actuation signal), CIAS (containment isolation actuation signal), MSIS (main steam isolation signal), AFAS (auxiliary feedwater actuation signal), CSAS (containment spray actuation signal), RAS (recirculation actuation signal).

The ESFAS comprising four identical protective channels can be roughly divided into three segments - bistables, logic matrices, and initiation circuits - as illustrated in Figure 1. There are many different types of plant process parameters associated with each ESF acuation signal, as shown in Table 1. Except for high-high containment pressure and low refueling water tank (RWT) level, all of parameters are shared with the reactor protection system (RPS). If an ESFAS trip is involved, the plant protection system (PPS) will transfer the appropriate ESF actuation signal into ESF components via the auxiliary relay cabinets (ARC) which consists of two trains. Also, the diverse protection system (DPS) comprising two protective channels can provide AFAS, independently.

Table 1. Plant Parameters Related to ESFAS functions

Parameters	ESFAS Functions
Low Pressurizer Pressure	SIAS, CIAS
Low Steam Generator (SG) Level	AFAS
High SG Level	MSIS
Low SG Pressure	MSIS
High Containment Pressure	SIAS, CIAS, MSIS
High-High Containment Pressure	CSAS
Low Refueling Water Tank Level	RAS

The KSNP 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.

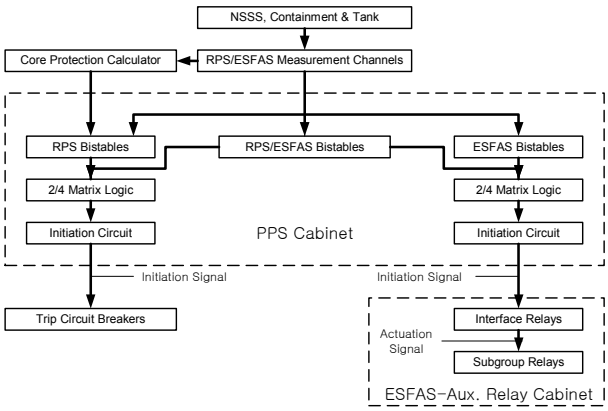

Figure 1. Simplified Block Diagram for the RPS and ESFAS in KSNP

3. System Fault Tree Analysis and Results

The top event of the ESFAS is described by 'no generation of ESF actuation signal on demand'. The fault tree of each ESF actuation signal was based on as-built/as-operated design of a KSNP. The fault trees cover measurement devices, bistables, bistable output relays, logic matrix relays, interposing relays, initiation relays, interface and subgroup relays in the ARC, signal processors and control circuits for the DPS, manual switches, and supporting system (e.g., electical system).

Generally, four types of data are required to quantify the system fault tree, namely, 1) 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 was used, which was estimated from the total operating experience of 8.63 commercial reactor years during a period of 1995 through 2000 at four units [1]. However, only a few of CCF events was found from the field data review, *e.g.*, multiple hunting of ex-core neutron flux chambers. So, insufficiency of CCF evidence led to use the generic data for CCF. The final CCF probabilities or rates were calculated by Beta-method, of which parameter values were obtained by the CEN-327[2]. They are distributed with a range of 0.02 to 0.1 depending on component type, for instance, 0.04 for bistable, 0.02 for logic matrix relay/contact, 0.1 for others, and so on.

Test and maintenance outages were modeled in the system fault tree. The average of test and maintenance outages was investigated by the interview with site staffs. Unavailabilities due to test and maintenance per channel were estimated to be about 4.0e-3 to 1.0e-4 for bistables (including measurement loop), 3.0e-4 to 5.0e-5 for logic matrices, 3.0e-3 for DPS, etc.

Two types of operator errors were considered in the fault tree: post-accident event (*e.g.*, failure of manual actuation) and pre-accident event (*e.g.*, miscalibration). The operator error probability was estimated by THERP [3]. The failure probabilities for manual actuation were ranged from approximately 0.001 to 0.004 for ESFAS. In particular, it was conservatively assumed that there was high dependency between miscalibration events for an input parameter.

The system fault trees were quantified using the KIRAP code [4]. The ESFAS unavailabilities with are summarized in Table 2, including the results of the uncertainty analysis. Except for the AFAS, the unavailabilities for other signals are estimated to be approximately 5.0e-6 through 7.3e-6, which are proportional to the number of the corresponding input parameters (refer to Table 1). Note that the unavailability of 1.8e-7 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, occupying the contribution of approximately 78% for MSIS and of 96% to 99% for the others. 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 contributors were CCFs coupled with failure of manual actuation by operator.

As a part of the sensitivity analyses on the system unavailability, the ESFAS fault trees were also quantified for two cases; 1) one channel is in bypass, and 2) additional one channel is in the failed condition. These are LCO's that are concerned in the current technical specifications for KSNP. The sensitivity results of these cases for the ESFAS unavailability are shown in Table 3.

Test and maintenance for a channel is generally placed in bypass, not a tripped mode. It means that one channel bypass (Case 1) brings an automatic change of the system operation mode from the two-of-four into the two-of-three coincidence logic. It leads to an increase of about three times or less than the system unavailability of the base case (Table 2). Plant may be continued in power operation under the current technical specification, even though additional one channel is placed in the tripped mode due to its inoperability (Case 2). It means that inoperability of additional one channel failure changes system operation from the two-of-three into the one-of-two logic. In this case, the system unavailabilities of the ESF actuation signals make additional increases of one-order or less than Case 1.

Table 2. Results of ESFAS Unavailability Analyses*

ESFAS Signals	Unavailability (Mean)	Uncertainty**		
		5%	50%	95%
SIAS	5.44e-6	3.54e-7	2.34e-6	1.93e-5
CIAS	5.44e-6	3.37e-7	2.31e-6	1.96e-5
CSAS	5.05e-6	2.16e-7	1.91e-6	1.89e-5
RAS	5.04e-6	2.13e-7	1.94e-6	1.93e-5
MSIS	7.24e-6	6.18e-7	3.64e-6	2.53e-5
AFAS	1.76e-7	6.06e-9	5.85e-8	6.77e-7

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

Table 3. Results of Sensitivity Analysis on the ESFAS

ESF Actuation Signals	Results of Sensitivity	
	Case 1*	Case 2**
SIAS	1.13e-5	9.88e-5
CIAS	1.13e-5	9.88e-5
CSAS	6.01e-6	3.09e-5
RAS	5.95e-6	8.10e-6
MSIS	2.64e-5	2.10e-4
AFAS	2.62e-7	2.45e-6

*) One channel is in bypass. **) Case 1, plus additional one channel is in trip condition.

3. Conclusion

The unavailability and sensitivity analyses of the ESFAS were performed on the plant-specific fault tree basis. The mean unavailability ranges from approximately 1.8e-7 to 7.2e-6 for each ESFAS signal train. The contribution of common cause failures reaches approximately 97% or more to the overall system unavailability. The results of the study, namely, ESFAS fault trees and plant-specific data can be useful for the risk-informed applications like the improvement of technical specifications.

ACKNOWLEDGEMENTS

This study was sponsored by the Ministry of Science & Technology (MOST). The authors would like to acknowledge the cooperation of the Korea Hydro and Nuclear Power Co. (KHNP) for data collection.

REFERENCES

[1] Jang, S.C., *et al.*, "Performance Analysis of the Safety Related I&C Components Based on Operational Experience during the Period of 1995-2000", KNS Spring Meeting, 2005.
[2] CE Owners Group, "RPS/ESFAS Extended Test Interval Evaluation," CEN-327, Combustion Engineering, 1986.
[3] Swain, A. D., and Guttmann,H. E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, U.S. NRC, 1983.
[4] Han, S. H., *et. al.*, "User's Manual for KIRAP Release 2.0, KAERI/TR-361/93, Korea Atomic Energy Research Institute 1993.