Fault Tree Modeling Using CBHRA and SAF Method

Korea Atomic Energy Research Institute
Hyun Gook Kang

Contents

1. Introduction

The Status of Nuclear Power Generation in Korea

NPP in Operation

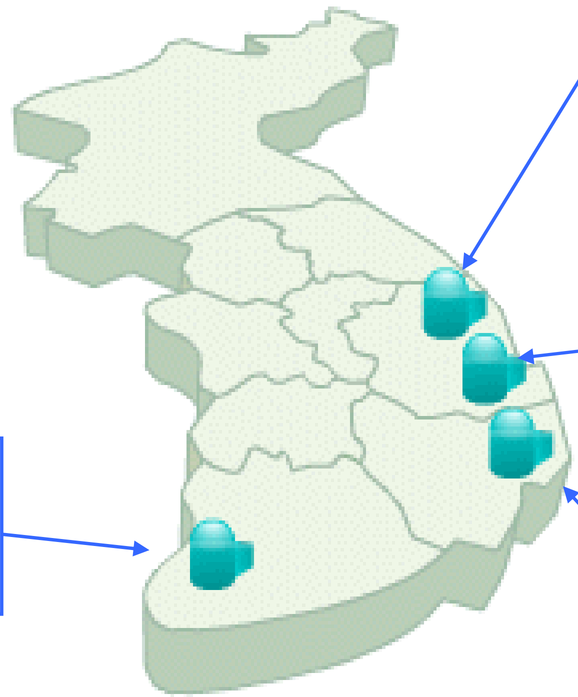
NPP in Planning

Ulchin
Nuclear Power Site
1, 2, 3, 4, 5, 6

Wolsong
Nuclear Power Site
1, 2, 3, 4

Shin-Wolsong #1, 2

Yonggwang
Nuclear Power Site
1, 2, 3, 4, 5, 6



Kori
Nuclear Power Site
1, 2, 3, 4

Shin-Kori # 1, 2, 3, 4

1. Introduction

- Digitalization of safety-critical functions in NPP
  - DPPS and DESFAS of Korean Nuclear Power Plants
  - Full digitalization in APR-1400

  → Increased importance of the digital I&C PSA
- Safety assessment (PSA) of NPP is essential
- Risk concentration on the digital system
  - Functional diversities might be useless since many functions share the same components and software
  - Redundancy in a digital system might be useless in the case of the CCF of the components
  - Digitalized system provides alarms and indications to the operator (the failure of another redundancy)

1. Introduction

The Status of I&C Systems in Korean NPPs

Systems / Plants	Reactor Trip System	ESFAS Systems	Protection Process	NSSS Control	PCS	Turbine Control	Main Control Board
Kori No. 1	Relay Logic (W/H)	Relay Logic (W/H)	Foxboro H-line	Foxboro H-line	Foxboro H-line	DCS	Conventional
Kori No. 1 (Upgraded in 1998)	Relay Logic (W/H)	Relay Logic (W/H)	Spec200 Spec200m (Foxboro)	Spec200 Spec200m (Foxboro)	Spec200 Spec200m (Foxboro)	DCS	Conventional
Kori No. 2,3,4 YG No. 1,2	SSPS Relay Logic (W/H)	SSPS Relay Logic (W/H)	7300 Analog	7300 Analog	7300 Analog	Mark V (GE)	Conventional
YGN No. 3,4	Relay Logic (ABB-CE)	Relay Logic (ABB-Œ)	Analog (ABB-CE)	Spec200 Spec200m (Foxboro)	ILS (Forney)	Mark V (GE)	Conventional
Ulchin No. 3,4 YG No. 5,6	Relay Logic (ABB-CE)	Relay Logic (ABB-CE)	Analog (ABB-CE)	Spec200 Spec200m (Foxboro)	PCS (Eaton)	Mark V (GE)	Hybrid
Wolsong No. 1,2,3,4	Relay Logic (AECL)	Relay Logic (AECL)	Analog/PDC (AECL)	DCC X/Y Computers Control	Analog/Relay (AECL)	Mark V (GE)	Hybrid
Ulchin No. 5,6	PLC (W/H)	PLC (W/H)	Analog (W/H)	Spec200 (PLC)	PCS (HFC)	Mark V (GE)	Hybrid
Shin Kori No. 1,2	PLC (W/H)	PLC (W/H)	Analog (W/H)	Spec200 (PLC) Ovation(W/H)	Teleperm XP (Siemens)	Mark VI (GE)	Hybrid
Shin Wolsong No.1,2 Shin Kori No. 3,4 (APR-1400)	PLC	PLC	Analog/PLC		PLC		Compact Workstation
HANARO Reactor	Relay Logic (AECL)	Not Applicable	Analog (AECL)	Control Computer	Not Applicable	Not Applicable	Hybrid

Reference: KINS

1. Introduction

- Since 1999, KAERI has performed an initiative research for the safety assessment of digitalized system in order to meet practical needs raised in Korea

- Careful treatment of CCF and HRA is required
  - Simplified alpha factor (SAF) method
  - Condition-based HRA (CBHRA) method

- Concurrent application of CBHRA of SAF methods
  - SAF technique may cause the loss of some information required for CBHRA

- Case study will be presented

2. Simplified Alpha Factor Method

- Alpha factor (Non-staggered test)

$$\alpha_k^{(m)} = \frac{n_k}{\sum_{i=1}^{m} n_i} = \frac{{}_m C_k * Q_k}{\sum_{i=1}^{m} ({}_m C_i * Q_i)}$$

  - Number of CCF events in the fault tree model for m-redundant component: $2^m - m - 1$
  - Multiple redundancy results in an impractically large number of CCF events in the fault tree model
- Simplified alpha factor method
  - Single CCF event represents the unavailability of system due to the CCFs of the specific redundant components
  - Assumption: the probabilities of CCF events are low enough

$$Q_{CCF} = \sum_{k=2}^{m} ({}_m C_k \times p_k Q_k^m) \qquad Q_k^m = \frac{k}{{}_{m-1} C_{k-1}} \cdot \frac{\alpha_k^m}{\sum_{i=1}^{m} i \cdot \alpha_i^m} \cdot Q_t$$

H.G. Kang, et al., The Common Cause Failure Probability Analysis on the Hardware of the Digital Protection System in Korean Standard Nuclear Power Plant, KAERI/TR-2908/2005

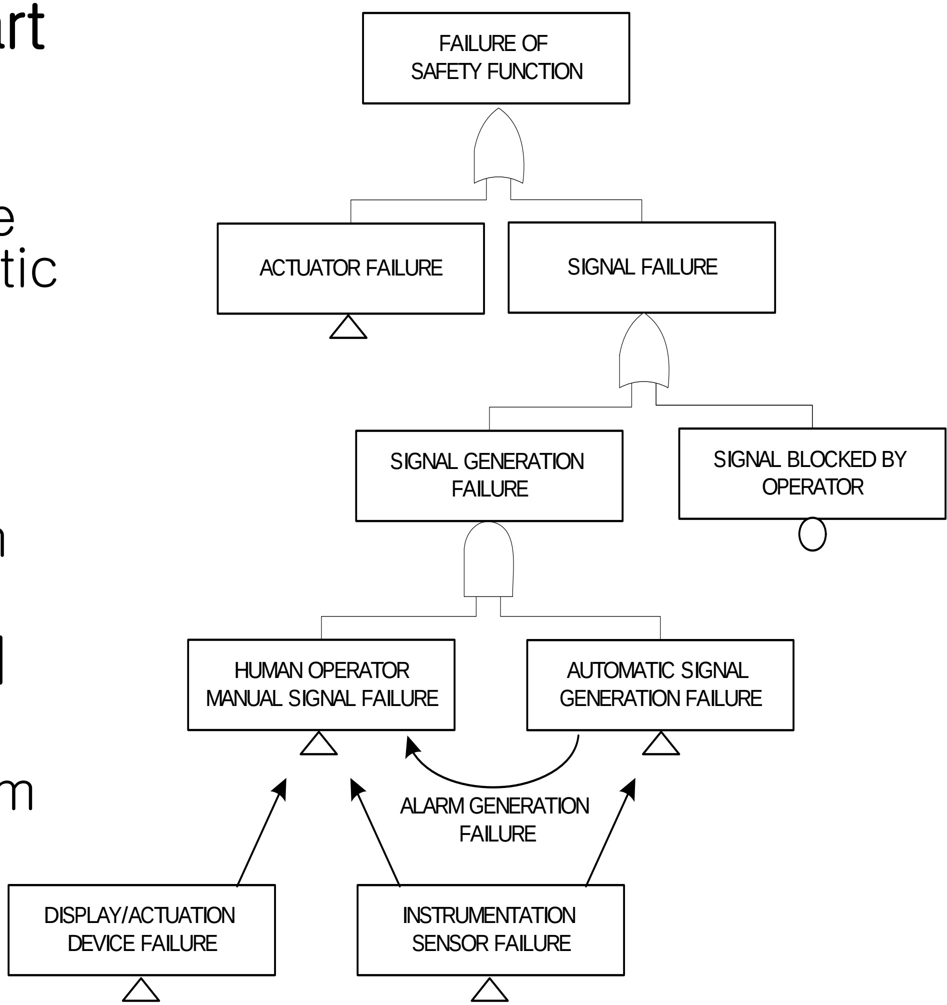
2. Simplified Alpha Factor Method

- Merits of SAF method
  - Complexity reduction of plant or system fault tree model
  - Quantification result is similar to that of detailed model
- Pre-processing for SAF method
  - Detailed success criteria and system design analysis

  → Determination of CCF boundary which causes the unavailability of the system
- Practical than the other methods
  - Simple fault tree than other full CCF event methods
  - Realistic results than other single CCF event methods
- The SAF method may cause the loss of some information required for the post processing of cutsets

3. Condition-based HRA

- Human operators are a part of the signal generation mechanism
  - Manual action plays the role of a backup for the automatic signal generation
  - The HEP of manual signal generation is a conditional probability given that the automatic signal generation fails
- Given condition of manual actuation
  - Failure of processing system
  - Unavailability of process parameters (sensors)



3. Condition-based HRA

- Conventional single event model for human error is not proper for this complicated case
- Condition-based human reliability assessment (CBHRA) method was proposed to address this problem in a practical way
  - CBHRA: A kind of post-processing of minimal cutsets (MCS) for treating the dependencies among the signal generation elements
  - Based on the events in the corresponding MCS, proper HEP which is predetermined is assigned

H.G. Kang and S.C. Jang, "Application of Condition-Based HRA Method for a Manual Actuation of the Safety Features in a Nuclear Power Plant", Reliability Engineering and Systems Safety, In press, 2005.

3. Condition-based HRA

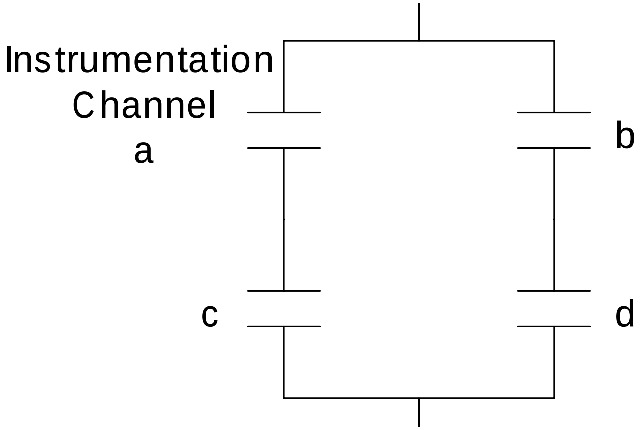
<CBHRA Steps>

(1) Conducting an investigation into possible EFCs
(2) Selecting important EFCs
(3) Developing a set of conditions in consideration of selected EFCs
(4) Estimating the HEP for each condition
(5) Constructing a fault tree which includes one human error (HE) event for each manual action
(6) Obtaining MCS by solving the fault tree
(7) Post-processing of MCSs based on the information from the events in a corresponding cutset

4. Case Study

- Target: DPPS (4-channel processing system)
  - System success criteria: selective 2/4
- Application of SAF method

Conceptual drawing



CCF Coefficient Calculation

No. of CCF channels (k)	${}_mC_k$	No. of system failure CCF (F_k)	p_k ($=F_k/{}_{16}C_k$)	Q_k / Q_t
1	4	0	0.000	-
2	6	2	0.333	0.0129
3	4	4	1.000	0.0092
4	1	1	1.000	0.0678
CCF coefficient (Q_{CCF} / Q_t)				0.1305

- System function failure CCF: {a,c}, {b,d}, {a,b,c}, {a,b,d}, {a,c,d}, {b,c,d}, {a,b,c,d}

4. Case Study

- Application of CBHRA method
  - Consideration of two Error Forcing Contexts (EFC)
    - Unavailability of alarms
    - Unavailability of indication of safety instrumentation channels

  → EFC = unavailability of information

  - Criteria of availability
    - Alarm: 2 or more alarms / 4 alarms
    - Indication: Case study variable
      - Case (A): 3 or more indications / 4 indications
      - Case (B): 2 or more indications / 4 indications
      - Case (C): 1 or more indications / 4 indications

4. Case Study

- Human errors under two different conditions
  - Condition 2: alarm unavailable, but indication available
  - Condition 3: alarm and indication unavailable

Status of instrumentation \ Status of the automated System	Normal	Abnormal
3 or more channels available	Auto. signal: O Indication: O Alarm: O *<Condition 1: EOC>*	Auto. signal: X Indication: O Alarm: X *<Condition 2>*
2 channels available	Auto. signal: O Indication: O/X Alarm: O *< Condition 1*: EOC>*	Auto. signal: X Indication: O/X Alarm: X *<Condition 2/3>*
1 channel available	Auto. signal: X Indication: O/X Alarm: X *<Condition 2/3>*	Auto. signal: X Indication: O/X Alarm: X *<Condition 2/3>*
No channel available	Auto. signal: X Indication: X Alarm: X *<Condition 3>*	Auto. signal: X Indication: X Alarm: X *<Condition 3>*

4. Case Study

- Case (A): 3 or more indications
  - The CCF does not affect on the categorization
  - CCF → <Condition 3>
- Case (B): 2 or more indications
  - The CCFs of {a,c} and {b,d} are included in the single CCF event
  - For the MCS which contains CCF event, two HE events :
    - {a,c} and {b,d} portion → <Condition 2>
    - The other portion → <Condition 3>

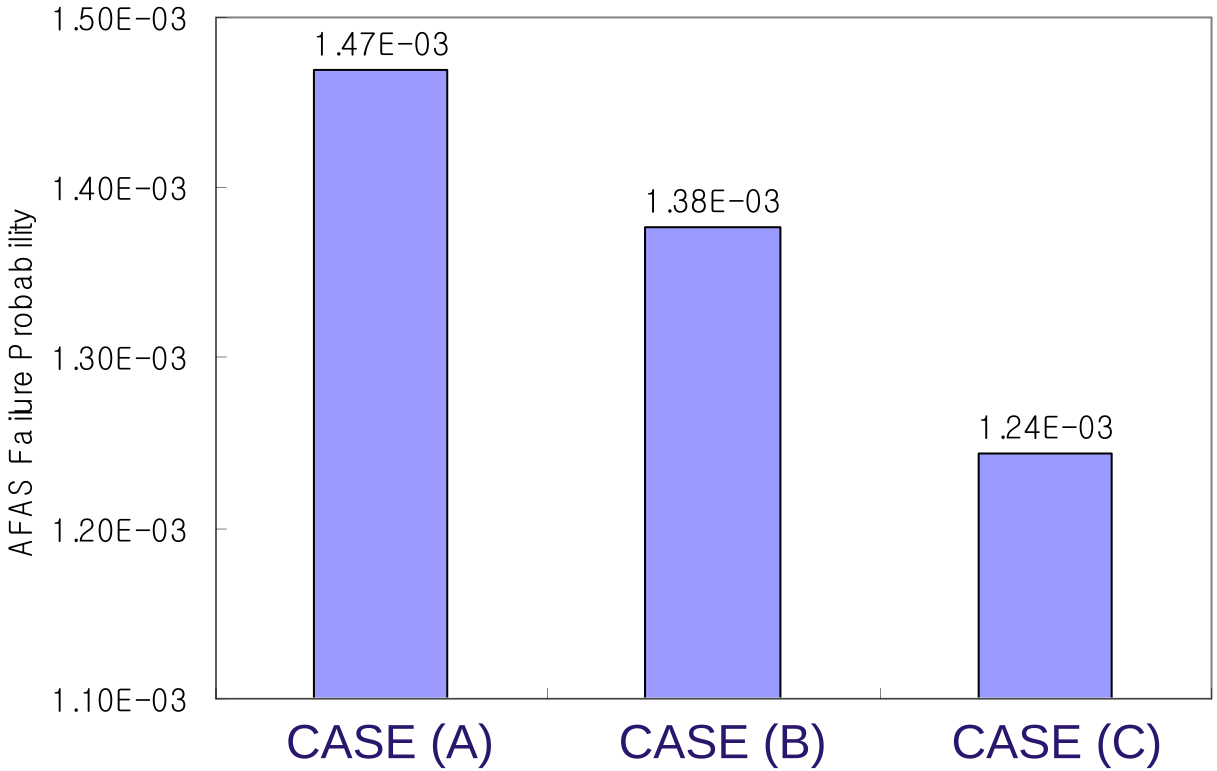
$$Q_{CCF-Condition2} = \sum_{k=2}^{2} ({}_4C_k \times p_k Q_k^4) \qquad Q_{CCF-Condition3} = \sum_{k=3}^{4} ({}_4C_k \times p_k Q_k^4)$$

- Case (C): 1 or more indications
  - {a,c}, {b,d}, {a,b,c}, {a,b,d}, {a,c,d} and {b,c,d}

$$Q_{CCF-Condition2} = \sum_{k=2}^{3} ({}_4C_k \times p_k Q_k^4) \qquad Q_{CCF-Condition3} = \sum_{k=4}^{4} ({}_4C_k \times p_k Q_k^4)$$

4. Case Study

- Results



5. Conclusion

- The single-event CCF modeling technique may cause the loss of system status information which is important in cutset analysis phase
- By using the same number of CCF events as that of human error conditions, the SAF method and the CBHRA method could be concurrently used without loss of accuracy
- The case study of the concurrent application of the SAF and the CBHRA method clearly demonstrates the usefulness of both method and the effect of EFC criteria determination