Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 10-11, 2007

Risk Effect Analysis of Digital Safety-Critical I&C System

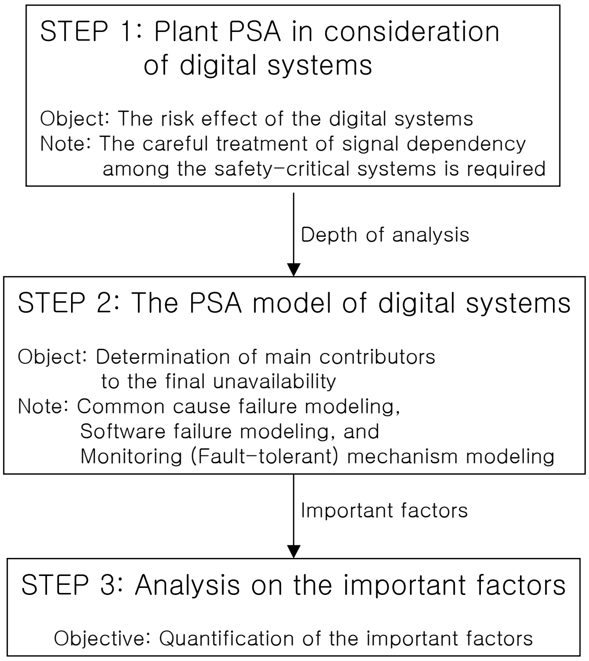
Hyun Gook Kang • Seung-Cheol Jang
Integrated Safety Assessment Team, Korea Atomic Energy Research Institute
P.O. Box 105, Yuseong, Daejeon, 305-600, Korea
hgkang@kaeri.re.kr

1. Introduction

UCN 5&6 nuclear units (OPR1000) are being constructed and the Korean Next Generation Reactor (APR1400) is being designed by using digital I&C equipment for the safety functions such as a reactor protection system, an engineered safety feature actuation system, and a safety equipment control system.

KAERI has performed safety assessment framework development by using conventional fault tree models. Even though the evaluation methods acceptable for some specific failure mechanisms in digital risk assessment (such as fault coverage, software failure probability) are not established yet, the trend analysis and rough risk effect analysis of digital safety-critical systems on a plant could be addressed based on the developed framework.

Authors had proposed a research plan and a systematic three-step approach for assessing the safety of digital systems in nuclear power plants in Kang and Sung [1] as shown in Figure 1. Each step in the proposed research approach should be iteratively performed based on the feedback from the results of the other steps. This article aims at presenting the first step based on the result of the second step. That is, we will address the importance of digital systems' failure to the plant-level safety. The result of primitive risk-effect analysis by using a simplified system model was presented in Kang et al. [2].


STEP 1: Plant PSA in consideration of digital systems

Object: The risk effect of the digital systems
Note: The careful treatment of signal dependency among the safety-critical systems is required

Depth of analysis

STEP 2: The PSA model of digital systems

Object: Determination of main contributors to the final unavailability
Note: Common cause failure modeling, Software failure modeling, and Monitoring (Fault-tolerant) mechanism modeling

Important factors

STEP 3: Analysis on the important factors

Objective: Quantification of the important factors

Figure 1. Steps for the safety assessment of digital safety-critical systems

2. Fault Tree Models

The fault trees for the digital systems, the Digital Plant Protection System (DPPS) and the Engineered Safety Feature Component Control System (ESF-CCS), are newly developed and integrated into the conventional OPR1000 risk model named the Risk Monitor developed by Korea Atomic Energy Research Institute. It consists of about 2176 basic events and 5464 logical gates.

The fault trees for the DPPS failure are constructed based on the information of the DPPS in Ulchin 5&6 nuclear units. And fault trees of the ESF-CCS are constructed based on the design data from APR1400 and KNICS ESF-CCS. It should be noted that the KNICS ESF-CCS in still in early design phase and the module failure probabilities are still in improving. Therefore, the models used in this study represent an interim design alternative.

That is, based on the Ulchin 3&4 plant model, we integrated the Ulchin 5&6 DPPS model and APR1400 ESF-CCS model as shown in Figure 2.

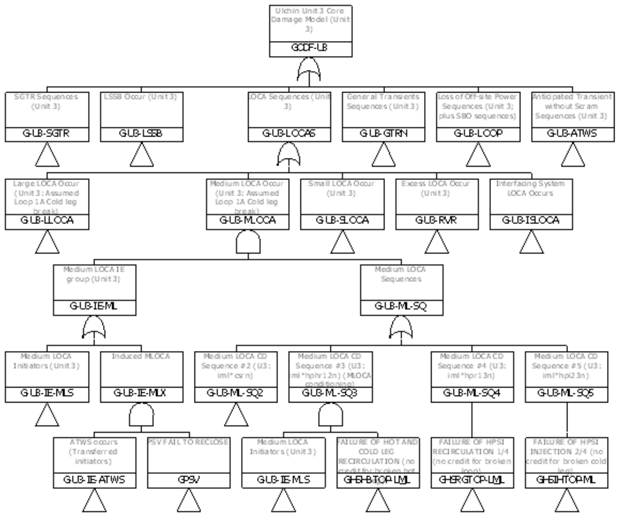

Ulchin Unit 3 Core Damage Model (Unit 3)
GCDF-LB
SGTR Sequences (Unit 3)
G-LB-SGTR
LSSB Occur (Unit 3)
G-LB-LSSB
LOCA Sequences (Unit 3)
G-LB-LOCAS
General Transients Sequences (Unit 3)
G-LB-GTRN
Loss of Off-site Power Sequences (Unit 3; plus SBO sequences)
G-LB-LOOP
Anticipated Transient without Scram Sequences (Unit 3)
G-LB-ATWS
Large LOCA Occur (Unit 3: Assumed Loop 1A Cold leg break)
G-LB-LLOCA
Medium LOCA Occur (Unit 3: Assumed Loop 1A Cold leg break)
G-LB-MLOCA
Small LOCA Occur (Unit 3)
G-LB-SLOCA
Excess LOCA Occur (Unit 3)
G-LB-RVR
Interfacing System LOCA Occurs
G-LB-ISLOCA
Medium LOCA IE group (Unit 3)
G-LB-IE-ML
Medium LOCA Sequences
G-LB-ML-SQ
Medium LOCA Initiators (Unit 3)
G-LB-IE-MLS
Induced MLOCA
G-LB-IE-MLX
Medium LOCA CD Sequence #2 (U3: iml*csrn)
G-LB-ML-SQ2
Medium LOCA CD Sequence #3 (U3: iml*hphr12n) (MLOCA conditioning)
G-LB-ML-SQ3
Medium LOCA CD Sequence #4 (U3: iml*hpr13n)
G-LB-ML-SQ4
Medium LOCA CD Sequence #5 (U3: iml*hpi23n)
G-LB-ML-SQ5
ATWS occurs (Transferred initiators)
G-LB-IE-ATWS
PSV FAIL TO RECLOSE
GPSV
Medium LOCA Initiators (Unit 3)
G-LB-IE-MLS
FAILURE OF HOT AND COLD LEG RECIRCULATION (no credit for broken hot leg)
GHEHBTOP-LML
FAILURE OF HPSI RECIRCULATION 1/4 (no credit for broken loop)
GHERGTOP-LML
FAILURE OF HPSI INJECTION 2/4 (no credit for broken cold leg)
GHEIHTOP-ML

Figure 2. Integrated model (top logic part)

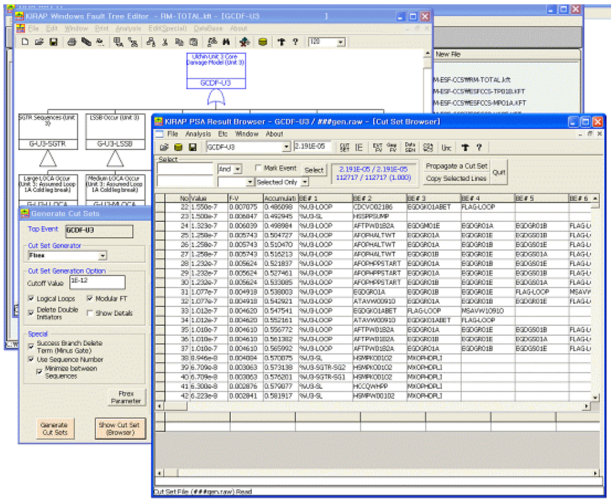
The modeling assumptions for the DPPS and the ESF-CCS fault trees could be briefly summarized as follows:

- Since we don't have enough information about the failure modes of digital systems, all the failure modes are assumed to be hazardous.
- For simplicity, we assume that the watchdog timers could detect software failures with the same coverage as in the case of hardware failures.
- We ignore the fail-to-hazard probability of the network communication protocol, the serial communications, and the inter-system data bus.
- We assume that the components are tested at least once per month.
- We ignore the effect of software failures.
- We assume very conservative values for the failure probability human operator.

3. Results of Quantification

3.1 Risk Classified by Initiating Events

Using AIMS which is the fault-tree analysis software package produced by the Korea Atomic Energy Research Institute, we analyzed the developed plant-risk models as shown in Figure 3. Risk profile over the initiating events can be illustrated as shown in Figure 4. Main contributors for the core damage frequency are the loss of offsite power event and the loss of coolant events (LL, ML, SL, SGTR). The risk profile is similar to the conventional plant risk analysis results.


KIRAP Windows Fault Tree Editor - RM-TOTAL.kft - [GCDF-U3]
File Edit Window Print Analysis Edit(Special) DataBase About
Ulchin Unit 3 Core Damage Model (Unit 3)
GCDF-U3
SGTR Sequences (Unit 3)
G-U3-SGTR
LSSB Occur (Unit 3)
G-U3-LSSB
Large LOCA Occur (Unit 3: Assumed Loop 1A Cold leg break)
G-U3-LLOCA
Medium LOCA Occur (Unit 3: Assumed Loop 1A Cold leg break)
G-U3-MLOCA
New File
M-ESF-CCS\RM-TOTAL.kft
M-ESF-CCS\ESFCCS-TP01B.KFT
M-ESF-CCS\ESFCCS-MP01A.KFT
Generate Cut Sets
Ftrex Parameter
Generate Cut Sets
Show Cut Set (Browser)
KIRAP PSA Result Browser - GCDF-U3 / ###gen.raw - [Cut Set Browser]
File Analysis Etc Window About
Select
Mark Event
Select
Propagate a Cut Set
Copy Selected Lines
Quit

Top Event: GCDF-U3
Cut Set Generator: Ftrex
Cut Set Generation Option
Cutoff Value: 1E-12
☑ Logical Loops ☑ Modular FT
☑ Delete Double Initiators □ Show Details
Special
☑ Success Branch Delete Term (Minus Gate)
☑ Use Sequence Number
☑ Minimize between Sequences

GCDF-U3 2.191E-05
And □ Mark Event Selected Only
2.191E-05 / 2.191E-05
112717 / 112717 (1.000)

No	Value	F-V	Accumulati	BE# 1	BE# 2	BE# 3	BE# 4	BE# 5	BE# 6
22	1.550e-7	0.007075	0.486098	%U3-LOOP	CDCVD02186	EGDGK01ABET	FLAG-LOOP		
23	1.500e-7	0.006847	0.492945	%U3-SL	HSSPPSUMP				
24	1.323e-7	0.006039	0.498984	%U3-LOOP	AFTPW0182A	EGDGM01E	EGDGR01A	EGDGR01B	FLAG-L
25	1.258e-7	0.005743	0.504727	%U3-LOOP	AFOPHALTWT	EGDGR01A	EGDGR01E	EGDGS01B	FLAG-L
26	1.258e-7	0.005743	0.510470	%U3-LOOP	AFOPHALTWT	EGDGR01A	EGDGR01B	EGDGS01E	FLAG-L
27	1.258e-7	0.005743	0.516213	%U3-LOOP	AFOPHALTWT	EGDGR01B	EGDGR01E	EGDGS01A	FLAG-L
28	1.232e-7	0.005624	0.521837	%U3-LOOP	AFOPHPPSTART	EGDGR01A	EGDGR01B	EGDGS01E	FLAG-L
29	1.232e-7	0.005624	0.527461	%U3-LOOP	AFOPHPPSTART	EGDGR01A	EGDGR01E	EGDGS01B	FLAG-L
30	1.232e-7	0.005624	0.533085	%U3-LOOP	AFOPHPPSTART	EGDGR01B	EGDGR01E	EGDGS01A	FLAG-L
31	1.077e-7	0.004918	0.538003	%U3-LOOP	EGDGR01A	EGDGR01B	EGDGR01E	FLAG-LOOP	MSAVW
32	1.077e-7	0.004918	0.542921	%U3-LOOP	ATAVW00910	EGDGR01A	EGDGR01B	EGDGR01E	FLAG-L
33	1.012e-7	0.004620	0.547541	%U3-LOOP	EGDGK01ABET	FLAG-LOOP	MSAVW10910		
34	1.012e-7	0.004620	0.552161	%U3-LOOP	ATAVW00910	EGDGK01ABET	FLAG-LOOP		
35	1.010e-7	0.004610	0.556772	%U3-LOOP	AFTPW0182A	EGDGR01A	EGDGR01E	EGDGS01B	FLAG-L
36	1.010e-7	0.004610	0.561382	%U3-LOOP	AFTPW0182A	EGDGR01B	EGDGR01E	EGDGS01A	FLAG-L
37	1.010e-7	0.004610	0.565992	%U3-LOOP	AFTPW0182A	EGDGR01A	EGDGR01B	EGDGS01E	FLAG-L
38	8.946e-8	0.004084	0.570075	%U3-SL	HSMPK00102	MXOPHDPLI			
39	6.709e-8	0.003063	0.573138	%U3-SGTR-SG2	HSMPK00102	MXOPHDPLI			
40	6.709e-8	0.003063	0.576201	%U3-SGTR-SG1	HSMPK00102	MXOPHDPLI			
41	6.300e-8	0.002876	0.579077	%U3-SL	HCCQWHPP	MXOPHDPLI			
42	6.223e-8	0.002841	0.581917	%U3-SL	HSMPW00102	MXOPHDPLI			

Cut Set File (###gen.raw) Read

Figure 3. Fault tree analysis using AIMS

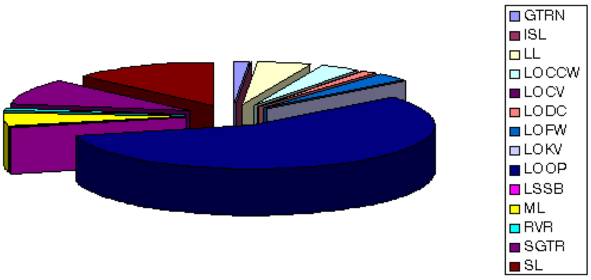


Figure 4. Risk classified by initiating events

3.2 Risk Contribution of DPPS and ESF-CCS

Based on the cutset analysis result, we found that the components in the DPPS and ESF-CCS contribute 10.33% of the core damage frequency. It includes the failure of human operator backup for the failure of automated reactor trip signal generation and the automated ESF components actuation. Main contributors are the human errors and the common cause failures of field instrumentation channels. In addition to that the common cause failures of the input, processor and output digital modules contribute large part.

4. Concluding Remarks

In conventional probabilistic safety assessments of nuclear power plants in Korea, we do not consider the failure of component control systems. In this study, in order to address the risk effect of digital systems in safety-critical applications in nuclear power plants, we developed an integrated model in consideration of automated component control systems. The results show that about one tenth of plant risk is caused by the DPPS and the ESF-CCS.

In order to get more precise results, the rough assumptions of this study should be refined.

Acknowledgement

This work has been carried out under the Nuclear R&D Program supported by MOST

REFERENCES

[1] Hyun Gook Kang and Taeyong Sung, "The Research Activities and Plan on The Risk Assessment of Digital I&C Systems in KAERI," The 7th Korea-Japan PSA Workshop, Cheju, Korea, 2002.

[2] Hyun Gook Kang, Seung-Cheol Jang and Jaejoo Ha, "A Simplified Risk Effect Analysis of Digital Reactor Protection System," Proceeding of KNS Autumn Conference, Yongpyoung, Korea, 2002.