Fault-tree modeling for the signal generation failures of the engineered safety features in digitalized nuclear power plant

H.G. Kang & S.C. Jang

*Korea Atomic Energy Research Institute, Daejeon, Korea*

ABSTRACT: A safety assessment for the engineered safety feature actuation system designed in the Korean Nuclear I&C System (KNICS) project by using newly developed safety-critical-class microprocessor-based modules was performed. Fault-tree models were developed to assess the failure probability of a system function which is to generate an automated actuation signal for accident-mitigation equipment. The quantification results show that the failures of digital output module, network module and processor module are dominant reasons for a system unavailability. The application of a redundancy in the signal generation system effectively improves the system function failure probability. Another important finding from this study is that a careful design of a manual actuation signal path is very important.

1 INTRODUCTION

1.1 PSA in nuclear applications

For the past several decades since the landmark reactor safety study (WASH-1400) was published in 1975, probabilistic safety assessment (PSA) techniques have been used to assess the relative effects of contributing events on a system-level safety or reliability. They provide a unifying means of assessing physical faults, recovery processes, contributing effects, human actions, and other events that have a high degree of uncertainty. Safety is the most important concern in the design and operation of nuclear power plants (NPPs). Currently, quantitative safety analysis is mainly performed in the framework of PSA. As the regulatory environment moves to a risk-informed regulation and application, PSA will become the basis for a lot of decision making for the operation of NPPs (Kim & Seong 2006).

PSA is also expected to provide useful tools for balancing safety, performance and cost since it provides information for the system under design. It means that as the PSA becomes more realistic, we can achieve a higher safety and economy.

The fault tree is the most familiar tool to PSA staffs. The logical and simple structure of a fault tree model also makes it easy for system design engineers to understand. In this study, we developed a fault-tree model for assessing the safety of a target system. Kim & Seong (2006) also pointed out that the PSA framework is well established, and therefore there is little controversy on its methodology if we apply it to a conventional target system. In this study, since the target system is a newly developed microcomputer-based safety-critical system, the unique features of a digital system should be considered carefully.

1.2 Safety-critical digital applications

In recent years many nuclear power plants have adopted modern digital I&C technologies since they are expected to significantly improve their performance and safety. OPR1000 in Korea (Korean standard nuclear power plant), typically Ulchin 5 & 6 nuclear units, have adopted safety-critical digital systems such as Digital Plant Protection System (DPPS) and Digital Engineered Safety Feature Actuation System (DESFAS), due to the functional advantages of smart digital systems and the obsolescence of the traditional analog components.

Currently, in Korea, there are several important industrial projects aiming at the development of digitalized safety-signal generation system for nuclear power plants. Among them, one of the most active research programs, Korean Nuclear I&C System (KNICS) project produced a new design the engineered safety feature (ESF) component control system (CCS) based on newly developed microprocessor-based modules. Notable advances of this ESF-CCS design are active applications of new technologies: the in-module-test mechanism, the hot-standby redundancy, and the network communication technology for safety signal generation.

PSA plays a very important role in proving the safety of a designed system. The usage of digital equipment in NPPs increases the importance of the development of risk evaluation technologies.
1.3 Important factors in the fault tree development of digital systems

The authors’ precedent studies (Kang et al. 2002, 2004) revealed that the coverage of a fault-tolerant mechanism and the software failure probability should be considered as very important factors which dominate the risk of a digital system. And proper modeling for the system design of ‘avoidance of common cause failure (CCF)’ also plays important role for a realistic fault-tree model development. The estimation of human operator’s failure probability is also one of the most dominant factors in the modeling of signal generation failures.

In this study, in addition to these factors, we will address the effect of network communication failure for each design alternative in consideration of a design strategy. The possible fault in communication protocol could be accommodated in the basic event of CCF of network modules. Since the data for estimating the failure probability of protocol is not available, the errors in a communication protocol are not considered in this study. We consider the hardware failures of the network modules only.

2 TARGET SYSTEM

2.1 ESF signals

In the case of an accident occurrence in a NPP, in order to mitigate the accident and maintain the nuclear reactor in safe status, there are several safety-feature-actuation signals in the OPR1000:

- Safety injection actuation signal (SIAS)
- Containment isolation actuation signal (CIAS)
- Containment spray actuation signal (CSAS)
- Recirculation actuation signal (RAS)
- Main steam isolation signal (MSIS)
- Auxiliary feedwater actuation signal-1 (AFAS-1)
- Auxiliary feedwater actuation signal-2 (AFAS-2)

These ESF signals are generated by a reactor protection system in the PPS. AFAS-1 and AFAS-2 signals could be generated by the diverse protection system (DPS) in addition to the generation by the PPS.

2.2 KNICS ESF-CCS layout

When an ESF signal is generated by the PPS, the ESF-CCS provides an automatic manipulation of the corresponding ESF components which consist of safety pumps and valves. That is, the ESF-CCS utilizes the bistable trip functions and coincidence logic in the plant protection system (PPS).

The ESF-CCS includes input, processor, output and network modules. Input modules interface with the ESF initiation signals from the PPS. Output modules transfer the actuated automatic control signal to the field component.

The processor modules in the ESF-CCS system can be categorized into two levels: Group controller and loop controller. A group controller performs an auctioneering by using four channel outputs from the PPS. If a specific ESF signal is generated based on the auctioneering results, the group controller provides information to the loop controllers. A loop controller which receives signal from the group controller generates control signal for the field components such as safety pumps and valves.

Figure 1 shows the conceptual layout of the KNICS ESF-CCS in one division. The ESF-CCS consists of four divisions. In each division, there are three group controllers and up to twelve loop controllers. Each loop controller has a hot-standby backup controller.

As described above, there are two redundant input sources of the ESF-CCS: the PPS and an operator. If the PPS successfully performs the function, it provides input to the group controller. The human operator could also manually actuate the field components as a backup of automated system (PPS) by providing a manual signal to the group controller. The group controllers provide the signal to the loop controllers via network communication. The group controllers’ signals are processed in a loop controller based on two-out-of-three voting logic. When a loop controller receives more than two actuation signals, it generates the control signal for the field components in consideration of the characteristics of each component. If the failure of a loop controller is detected by the group controller, the backup controller of corresponding group controller will take over the task.

In order to reduce the failure probability of the field components’ control signal, there are two more sources in addition to the loop controller of the ESF-CCS. The DPS is an independent and separated automatic system for signal generation. Diverse manual actuation provides a redundant mean for the operator in the main control room to access the field components via hardwired path. It is notable that the DPS and the diverse manual actuation switches do not cover all the field components. Each of these redundancies provides a safety signal to a limited number of components only.

3 FAULT TREE MODEL

3.1 Modeling assumptions

The assumptions used in the model can be summarized as follows:

- Since we don’t have enough information about the failure modes of digital systems, all failure modes are assumed to be hazardous.
– The input signal from the PPS is assumed to be generated by using the reactor protection system developed by the KNICS project.

– Since post action after a watchdog timer (WDT) detects a failure is not decided, the possibility of fail-safe state due to the WDTs which detect the failure of controllers is ignored.

– Generally, the fault coverage of processor-to-processor (PTP) monitoring is much higher than that of WDT monitoring because the PTP monitoring method usually adopts much more sophisticated algorithms. Since the coverage of WDT monitoring could be assumed around 0.5 (Kim et al. 2006), we assume that the PTP monitoring coverage is 0.9.

– We ignore the probability of software failure in the controllers.

– If a failure of network communication occurs, a controller is assumed to fail to detect the failure of other controller(s).

– The loop controllers are assumed to fail when they lose the communication with the group controllers. That is, when demand arrives (accident occurs), if a failure of network communication occurs, group controllers cannot transmit a demand signal to loop controllers.

– We ignore the fail-to-hazard probability of the inter-system data bus and the back plane of PLC.

– We assume that the components are tested at least once per month. That is, the periodic test interval (T) is 720 hours. Component unavailability (Q) is the half of the product of failure rate ($\lambda$) and periodic test interval: $Q = \frac{\lambda T}{2}$. And we ignore the effect of automatic tests.

The aim of this study is to investigate the risk from the newly developed system and to improve the unavailability of the system based on the quantitative analysis. So even though the adequacy of these assumptions is not guaranteed and the model requires further refinement, the results of the PSA and sensitivity studies could provide useful insights.

3.2 Data

For the newly developed digital modules by the KNICS, we use their failure probability data from a KNICS design document (Choi 2004). For the conventional analog equipment and sensors, the generic data updated by KAERI (Min 2002) is used.

3.3 Fault tree development

The fault tree is constructed and the minimal cut sets (MCSs) are determined by using the KIRAP, an integrated safety assessment software package developed at KAERI. As mentioned above, there are many filed
components which should be operated when one or more ESF signals are generated. In this study, the top event of the model is 'the failure of an ESF signal generation'. Figure 2 shows one of the developed fault tree model. It is a top logic of the fault tree which models the AFAS-1 signal failure for a typical field component, MP01A.

4 QUANTIFICATION AND ANALYSIS

In this study, we performed a quantification for three typical cases:

– Case 1: Single sensor train provides input to the PPS for safety signal. The DPS does not provide redundant signal for actuating the component.

![Fault Tree Diagram](image-url)

Figure 2. Top logic of the developed fault-tree model of KNICS ESF-CCS (AFAS-1 signal failure for a field component, MP01A).
– Case 2: Two sensor trains provide input to the PPS for safety signal. The DPS does not provide redundant signal for actuating the component.
– Case 3: Single sensor train provides input to the PPS for safety signal. The DPS provides redundant signal for actuating the component.

When we ignore the diverse manual actuation, the quantification results can be summarized as in Table 1.

Table 1. The quantification results of typical examples (Case 1, Case 2 and Case 3) without the diverse manual actuation.

<table>
<thead>
<tr>
<th></th>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESF signal</td>
<td>RAS</td>
<td>SIAS</td>
<td>AFAS-1</td>
</tr>
<tr>
<td>DPS</td>
<td>X</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Input sensors</td>
<td>RWT level</td>
<td>Pressurizer pressure</td>
<td>Containment pressure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Steam generator level</td>
<td></td>
</tr>
<tr>
<td>Unavailability of</td>
<td></td>
<td>2.27E-3</td>
<td>2.34E-3</td>
</tr>
<tr>
<td>actuation signal</td>
<td></td>
<td></td>
<td>7.95E-5</td>
</tr>
</tbody>
</table>

Figure 3 shows dominant cutsets of Case 3. The important basic events in dominant cutsets are digital output module failures, sensor failures, DPS processor failures, CCF of network communication modules, processor module failures, and CCF of digital input modules.

If we consider the effects of a diverse manual actuation, and assume its failure probability as 0.1, the quantification results can be summarized as in Table 2. Note that the failure probability of manual action in Figure 2 is assumed to be 0.05. We also consider the dependency between these two human actions. Once the operator fails to initiate the signal (failure of manual actuation), then we do not give credit to the diverse manual actuation since the diverse manual actuation for each component is much more complicated task than the manual actuation of ESF signal.

Usually, the failure probabilities of active components such as pumps and valves are higher than 1.0E-3. The quantification results in Table 1 show that the failure probabilities of safety signals are quite high in consideration of those of the active components. On the other hand, from the results in Table 2, we can find...
Table 2. The quantification results of typical examples (Case 1, Case 2 and Case 3) with the diverse manual actuation of which failure probability 0.1.

<table>
<thead>
<tr>
<th></th>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESF signal</td>
<td>RAS</td>
<td>SIAS</td>
<td>AFAS-1</td>
</tr>
<tr>
<td>DPS</td>
<td>X</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Input sensors</td>
<td>RWT level</td>
<td>Pressurizer pressure</td>
<td>Steam generator level</td>
</tr>
<tr>
<td>Unavailability of actuation signal</td>
<td>2.78E-4</td>
<td>3.49E-4</td>
<td>9.71E-6</td>
</tr>
</tbody>
</table>

The quantification results show that the actuation signal failure probability of safety signal in a NPP is low enough if the diverse manual actuation is considered. The result implies that the careful design of manual actuation signal path is very important. If the operators manipulate field components directly and they are well trained for this task, the risk from signal failure could be reduced in an effective manner.

5 CONCLUSION

In this study, a safety assessment for the KNICS ESF-CCS was performed. Since the ESF signals from the ESF-CCS play a very important role in mitigating possible damage from an accident, the safety of the ESF-CCS is very important. Based on the fault-tree models developed to assess the failure probability of the ESF signal generation, we performed quantification of unavailability of actuation signal for active field components.

The quantification results show that the important basic events in dominant cutsets are the digital output module failures, the sensor failures, the DPS processor failures, a CCF of the network communication modules, the processor module failures, and a CCF of the digital input modules.

For the ESF signal generation, there are two more signal sources in addition to the ESF-CCS. Without these diversities the failure probabilities of the ESF signals are too high to use in safety-critical application in NPPs. The quantification results show that the application of diversity in the automatic signal generation system (DPS) effectively improves the signal failure probability. Another important finding from this study is that the careful design of manual actuation signal path is very important. If we successfully provide means to the operators for manipulating field components directly, the risk from signal failure would be reduced in an effective manner.

ACKNOWLEDGMENT

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

REFERENCES

Choi, J.K. 2004, RPS unavailability analysis, KNICS-RPS-AR103. Rev. 02, Korea Atomic Energy Research Institute