Development of Safety Assessment Tool During Outage of CANDU Plants

Hae Cheol Oh, Myung Ki Kim, Bag Soon Chung, Myung Suk Sung, Sung Yull Hong
Korean Electric Power Research Institute., 103-16.,Moonjidong., Yusung-Gu., Daejeon, haech@kepri.re.kr

1. Introduction

As a part of a National Nuclear Technology Program of Ministry of Science & Technology (MOST), KEPRI is developing a defense-in-depth model to monitor risk during the planned outage for CANDU reactors. To have a better knowledge of the safety assessment using defense-in-depth model, a safety assessment process has been developed and applied to a practical event occurred in any CANDU plant. This approach is described herein briefly, and the result of the example evaluation is presented.

2. Safety Assessment Method During Outage

Nuclear reactor operating experience has shown that plants can be subject to a variety of events during shutdown operation that pose potential safety challenges. These events do illustrate that careful attention to both outage management and operator preparedness is necessary to maintain defense in depth during shutdown operation. The intent of the safety assessment is to identify the risk potential of various phases of an outage and to determine actions that the operators or schedulers can take to minimize risk.

In this section some of the techniques used to evaluate safety status for the plant configuration are described.

2.1 Safety Function Assessment Trees

The Safety Function Assessment Trees (SFATs) evaluate defense-in-depth associated with key plant safety functions for each plant configuration. These SFATs related the number of safety systems available to discrete end-states. Each end-state is represented by a color that qualifies the degree of defense-in-depth for the safety function. The logic which generates the safety function is based primarily on Technical Specifications. The SFATs uses the results of system fault trees and plant configuration database variable to determine the configuration safety level. This configuration identification information includes the individual maintenance activities imported from the outage schedule program. The defense-in-depth is measured by number, redundancy and diversity of systems, structures, and components (SSCs) which are needed to mitigate challenges to the safety functions Even though the fault trees are used, SFAT are typically deterministic in nature and the reliability may not be explicitly addressed, risk insights can be used however.

In order to develop outage defense-in-depth model, first of all, safety functions for outage operations should be defined. In NUMARC 91-06, safety functions for shutdown and outage operation are defined as Residual Heat Removal, Inventory Control, Reactivity Control, Containment Integrity, Power Availability. Residual Heat Removal safety function can be divided into two area of shutdown cooling in RCS and shutdown cooling in SFP generally. For example, Inventory Control safety function concerns the SSCs required to mitigate LOCA. Once safety functions are defined and SFATs are constructed, the impact of each safety function due to test and maintenance can be evaluated automatically through SFAT.

2.2 SFAT example application

A safety assessment process was applied for practical event occurred in other country's CANDU plant.

This event was a loss of primary heat sink while shutdown. The event description is given as the following. During a maintenance outage on any CANDU plant, the reactor was in the guaranteed shutdown state and the PHT system in the low level drained state. Header levels were then reduced further to perform inspection on ECCS check valves. Concurrent with that work, the bleed condenser and the pressurizer were being drained for maintenance on the pressurizer steam bleed valves and PHT interconnect valves. The conditions were passed over to the next shift. With the bleed condenser empty, stroking of the first LRV caused a drop in outlet header level sufficient to expose the suction line to the shutdown cooling system pumps, causing the running pump to gas lock. Coolant flow stopped immediately but was not noticed for a period of about two hours. The LRV's remained open 15 minutes after the loss of flow was realized, diverting more coolant to the bleed condenser. Venting of the SDC pumps was difficult. As a precaution, preparations to establish the back up heat sink were initiated one hour after it was discovered flow had been lost (See Figure 1).

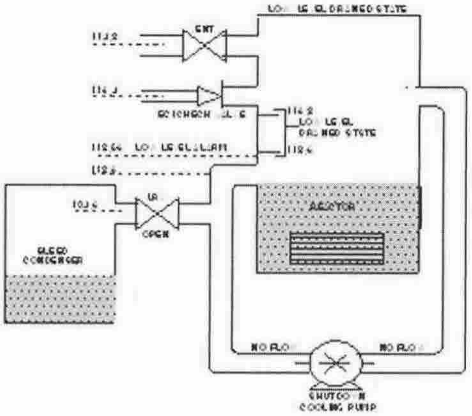


Figure 1. Loss of Shutdown Cooling at any CANDU Plant

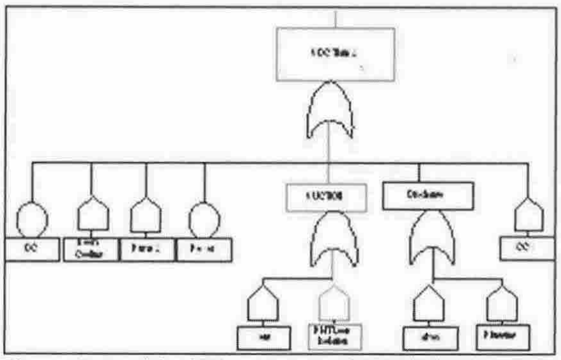


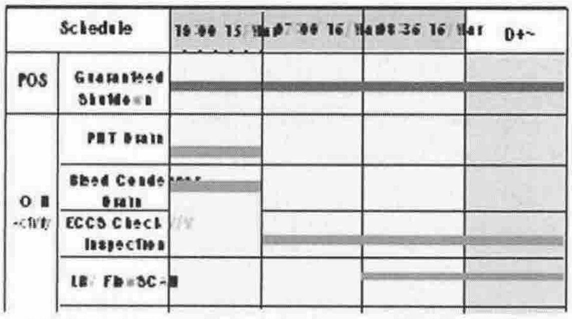
Figure 2. Residual Heat Removal SFATfor CANDU Plant

2.3 SFAT evaluation

This event is checked with Residual Heat Removal (RHR) SFAT and Inventory Control SFAT for CANDU plant.

The outage schedule described in section 2.2 is presented as Table 1. If this schedule is imported into the RHR SFAT, The overall results will be red color automatically as shown in Figure 2.

SDC Loop isolation failure due to LRV open with the empty of bleed condenser cause a loss of both SDC trains. This is shown in Figure 3. From this result, zero SDC path in figure 2 will be selected. If the operation or maintenance personnel had been performed the review work with this tool before the outage or during outage, They would have changed the LRV test schedule and loss of SDC such as this event could be prevented.



Schedule		19:00 15/Mar	07:00 16/Mar	08:36 16/Mar	D+~
POS	Guaranteed Shutdown	▨	▨	▨	▨
O R -ctivity	PHT Drain	▨			
	Bleed Condenser Drain	▨			
	ECCS Check Inspection		▨	▨	▨
	LR[illegible]			▨	▨

Table 1. Outage Schedule for any CANDU Plant

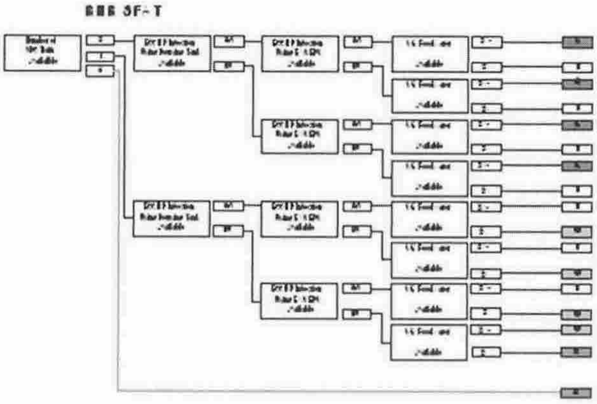


Figure 3. Shutdown Cooling Fault Tree for CANDU Plant

3. Conclusions

The technique of safety function assessment tree (SFAT) was introduced and the evaluation example with real one was presented. After the completion of this project, an easy safety review with the defense-in-depth tool can be done prior to each outage, and before each major change of state in the outage. Safety assessment techniques using defense-in-depth approach can be useful tools for scheduling of the outage.

REFERENCES

[1]NUMARC, Guidelines for Industry Actions to Assess Shutdown Management, NUMARC 91-06, December 1991.

[2]ORAM-SENTINEL TM, USER's Manual,Version 3.0, EPRI, Palo Alto, CA. TR-107018, 1997.

[3]The proceeding of 4th Technical Committee Meeting on The Exchange of Operational Safety Experience of PHWRs. 1996.