Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 27-28, 2016

Assumptions and Policy Decisions for Vital Area Identification Analysis

Myungsu Kim *, Yeon-kyoung Bae, Youngseung Lee
Korea Hydro & Nuclear Power Co., Ltd., Central Research Institute
70 1312 beon-gil, Yuseong-daero, Yuseong-gu, Daejeon, 305-343, KOREA
Corresponding author: enchanted@khnp.co.kr

1. Introduction

U.S. Nuclear Regulatory Commission and IAEA guidance indicate that certain assumptions and policy questions should be addressed to a Vital Area Identification (VAI) process [1].

Korea Hydro & Nuclear Power conducted a VAI based on current Design Basis Threat and engineering judgement to identify APR1400 vital areas. Some of the assumptions were inherited from Probabilistic Safety Assessment (PSA) as a sabotage logic model was based on PSA logic tree and equipment location data.

This paper illustrates some important assumptions and policy decisions for APR1400 VAI analysis.

2. Applied Assumptions and Policy Decisions

2.1 Radioactive material in a nuclear power plant

In order to prevent radiological sabotage of a nuclear power plant, it is necessary to prevent significant core damage and spent fuel sabotage. Vital areas should be identified so as to protect a minimum set of the systems, personnel, and equipment needed to prevent significant core damage and spent fuel sabotage.

During review process, it was noticed that systems for liquid, gaseous, solid radioactive waste treatment should be evaluated for radiological sabotage. It was discussed that direct dispersal from these systems should be determined. This issue can be traced up to threat assessment and DBT. It is less likely to target a nuclear power plant to get a chance for acquiring radioactive material from radioactive waste processing systems, and also attack those systems when they already gain access to nuclear power plant.

2.2 Distinct operating states

All distinct operating states (power operation, hot standby, cold standby, and refueling) should be addressed in the vital area identification.

Different operational states may rely on different equipment to perform safety functions and require protection of different areas to ensure protection against sabotage. A set of vital areas may be identified for each operational state or a bounding set of vital areas that provides protection during all operating states can be selected. Optimal sets of vital areas were derived from sabotage logic model analysis and expert panel discussions for different operational states.

2.3 Random failure and maintenance for equipment

It is not necessary to assume that a random failure of vital equipment occurs concurrently with an attack. A philosophical background for not crediting random failure in sabotage scenario is that saboteurs do not rely on their success that can be accomplished by luck of equipment availability; rather they would make sure their targets are damaged for sure.

The system fault trees developed for PSA frequently include events that do not involve equipment, component, or device faults, but affect system reliability or availability. Non-fault events of this type include operator recovery actions, test and maintenance outages, and human errors.

In building logic models for the VAI analysis, it is not necessary to assume that a vital equipment maintenance outage occurs concurrently with an attack. Vital equipment maintenance outages that occur during operations should be addressed and may require the implementation of compensatory measures. Reviewing VAI results, it was pointed that some vital equipment should be designated and protected as alternate vital areas containing redundant equipment.

2.4 Operator actions and initial conditions

Not all of operator actions were taken to be credible

for operator actions. Only limited actions were counted based on the location of commencement.

It was assumed that a loss of offsite power (LOOP) occurs concurrent with an attack.

It is also important to assume that all equipment outside the protected area of the plant is lost unless continued operation of the equipment makes the situation worse. This naturally concludes that water storage tanks and equipment in yards without any structural protection cannot be guaranteed to survive during sabotage.

3. Decisions to be made for further studies

Through APR1400 VAI process, it was notice that there are some more assumptions and policy decisions to make in order to analysis more realistic, and gain mutual understanding from engineers, plant operators, and regulators at the same time.

One of the main issues is “mission time”. The PSA Standard defines mission time as “… the time period that a system or component is required to operate in order to successfully perform its function.” [2] It is suggested that for sequences in which stable plant conditions have been achieved, use a minimum mission time of 24 hours[3]. For sabotage scenarios, it is not practical to assume any kind of conflict would last that long when sabotage occurs. Plant response should be efficient enough to naturalize adversaries with in a limited time. Including that as a limitation of threat, event tree logics from PSA can be modified, so that number of vital areas would reduce and reasoning for target sets should be simpler and more agreeable. However defining mission time for sabotage itself is a hard topic to conclude, also modifying PSA event tree would not be easy without detailed thermo-hydraulic analysis.

4. Conclusions

Assumptions and policy decisions could be overlooked at the beginning stage of VAI, however they should be carefully reviewed and discussed among engineers, plant operators, and regulators.

Through APR1400 VAI process, some of the policy concerns and assumptions for analysis were applied based on document research and expert panel discussions.

It was also found that there are more assumptions to define for further studies for other types of nuclear power plants. One of the assumptions is mission time, which was inherited from PSA. However, we noticed that PSA and VAI should not use same mission time, so that the VAI result can be more realistic.

REFERENCES

[1] Sandia National Laboratories, Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants, SAND2008-5644, 2008

[2] American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2005, 2005

[3] U.S. Nuclear Regulatory Commission, Risk Assessment of Operational Events Handbook, Volume I, Internal Events, Revision 1.03, 2009