Proceedings of the Korean Nuclear Society Spring Meeting
Cheju, Korea, May 1996

Trends in Risk Management and Accident Management in Nuclear Industry

Inn Seock Kim*
Korea Atomic Energy Research Institute

Abstract

Safety management may be classified into three dimensions: (1) risk management, (2) accident management, and (3) emergency management. This paper addresses the recent trends of safety management in nuclear industry, focussing on risk management and accident management.

1. Introduction

The top objective of a nuclear power plant is to maximize its availability and safety. High availability of the plant will be achieved by reducing failure rates of the plant equipment, or inadvertent trips of the plant. On the other hand, the plant's safety can be maximized by properly managing the safety before, during, after an accident.

As articulated in a study sponsored by the US Nuclear Regulatory Commission, [1] one may call the safety management before, during, after an accident, risk, accident, emergency management, respectively. These three different types of safety management relate to the role of the operating crew and the technical support provided to them.

An elaborate definition of these three important terms, classifying the safety management, has been made in Ref. 1 as follows:

1) Risk management: That ensemble of analysis, decisions, and actions taken to optimize risk.
2) *Accident management*: That set of actions taken by the plant operating crew to gain control of the outcome of an abnormal event at the earliest possible time and with the minimum adverse consequences.
3) Emergency management: That ensemble of analyses, decisions, and actions taken to protect the public from suffering the effects of a potential or actual release of radioactive material from the site.

This paper briefly discusses the recent trends in these three different activities of safety management.

---

*Visiting Scientist under the Brain Pool Program of Korean Government

The emphasis is placed on risk management and accident management.

2. Risk Management

The term risk means the possibility of suffering harm or loss. As applied to nuclear power, the risk mainly stems from the great amount of radioactivity and the process environment of high temperature and high pressure.

Considerable research is underway to assess the risk associated with the operation of nuclear power plants. The probabilistic risk assessment (PRA), or sometimes called probabilistic safety assessment (PSA), is increasingly used to assess the risk associated with the operation of a nuclear power plant. The PRA assesses the plant's risk by logically modeling the potential accident sequences in terms of event trees, with the system unavailabilities estimated in terms of fault trees. The risk is quantified by applying the empirical data of the plant, generic or plant-specific, to the logic models.

Shutdown risk, i.e., the risk associated with shutdown operation of the nuclear plant, such as midloop operation or hot shutdown operation, oftentimes has been considered negligible compared to the risk during full-power operation. However, the operating experience of nuclear plants, and also the subsequent analysis, suggested that the plant risk during such shutdown modes is not insignificant.

The assessment of risk, whether from power or shutdown operations, addresses

1) What can go wrong?
2) How likely is it?
3) What are the consequences?

Hence, we can express the risk as:

$$Risk(i) = Frequency(i) * Consequence(i)$$

The total risk is the sum of the risks from all the accident scenarios for the plant.

An accident scenario consists of:

$$IE(i) * HW(j) * HW(k) * HW(l) * NR(m)$$

where IE represents an initiating event, HW an event of hardware failing to respond to the initiator, NR an event of the operator failing to recover the abnormal situation.

Hence, three basic elements constitute accident sequences; namely, (1) initiating events, (2) hardware responses, and (3) human errors or non-recovery actions. The initiating events may occur internally or externally; for example, internal events such as loss of main feedwater, and external events like earthquake or flooding.

Thus far, the nuclear community mainly focussed on assessing the risk impact associated with the operation of nuclear power plants. There now is a growing interest in managing the plant's risk using the models developed in the PSAs. Risk management includes such activities as:

1) PSA application to improve technical specification requirements

2) Development of an on-line risk monitor

3) Prioritization of maintenance acts based on relative risk importance

4) Prioritization of plant inspections based on relative risk importance

5) Control of the plant configurations from the overall risk perspective

Much research has been carried out particularly in the U.S. to develop PSA-based methods for the risk management.[2] However, as a former chairman of the US Nuclear Regulatory Commission clearly stated, PSA has three limitations among others: [3]

1) PSAs are not yet reliable overall indicators of absolute levels of safety

2) PSAs are not yet replicable enough to compare the relative safety of one nuclear installation to another

3) PSAs are not yet replicable enough to use as the basis for regulations

In spite of these limitations, PSAs have a great deal of merits. For instance, PSAs give us an excellent idea of the relative weaknesses in a defense in depth, of the vulnerabilities of a system, and of the areas where safety emphasis should be put. [3] As a result, the USNRC also has decided to use PSAs or risk-based methods to facilitate decision making associated with regulatory processes. [4]

Another thing to mention in relation to risk management is man-machine interface (MMI). Much work is being carried out worldwide to improve the MMI of nuclear power plants. For example, the human engineering deficiencies in conventional control rooms are identified and fixed to reduce potential human errors or to improve the operator's recovery capability.

The enhancement of MMI also is a part of risk management, as well as of accident management to be discussed below. In fact, a study has indicated that the plant's risk is very sensitive to human errors, and as a result, a reduction in human errors or an improvement in human reliability will significantly help to reduce the plant risk.

3. Accident Management

Accident management has two different aspects:

1) Accident prevention

2) Accident mitigation

An accident typically starts from a small incident, e.g., the penetration of water into the instrumentation system at the TMI-2 nuclear plant. If the operating crew terminate it or restablize the process before its propagation into a serious event, they can prevent an accident from occurring. However, should an accident occur, all they can do is mitigate it to minimize the adverse consequences.

The major role of managing an accident is on the shoulders of the control-room operators of the plant who are the supervisors of the plant process through the man-machine interface (MMI). A provision of an appropriate MMI for the operators is thus extremely important for accident management, because it is a main

source of information about the plant situation, and furthermore, it provides a vehicle by which the process can be controlled.

Modern computer techniques, such as artificial intelligence, knowledge-based systems, integrated graphic displays, soft controls, and computer-driven large dynamic graphic displays, are increasingly used for the MMI of advanced nuclear power plants. Computerized alarm annunciator systems and diagnostic systems also tend to apply knowledge-based AI techniques.[5]

Another notable trend in regard to the MMI improvement in nuclear power plants is a wide application of human factors engineering, where human factors deficiencies are identified and corrected and the opinions of the end-users (e.g., the main control-room operators or the technical supervisory staff) are reflected in the design of the MMI systems intended for their use.

These new trends of accident management are desirable. For example, the improved MMI will help the operators better assess the plant situation, and as a result, less likely to make a misdiagnosis which can have a serious impact on the plant's operational safety, as in the TMI-2 accident.

More specifically, the MMI systems under development include

1) Computer-based alarm annunciator systems
2) On-line process surveillance and diagnosis systems
3) Sensor validation systems
4) EOP (emergency operating procedure) tracking systems

The computerized alarm annunciator systems attempt to reduce the number of alarms presented to the operator during a major plant upset, by prioritizing the alarm messages based on a certain logic. In fact, the enormous alarm data in the first several minutes during the TMI-2 accident were rather a nuisance than a help to the operating crew.

Great efforts have been spent on enhancing the alarm annunciator system. However, most operating plants are still equipped with conventional alarm panels, containing more than a thousand alarm tiles. Hence, there is still a possibility of the alarm avalanche being repeated, should a major plant upset ever occur.

Most of other MMI systems mentioned above, such as on-line process monitoring and diagnosis systems, are still in a development stage, although some, such as the Early Fault Detection (EFD) system of the Halden Reactor Project, have been implemented and tested against a real process environment. [5]

For management of severe accidents involving degraded core or core damage (i.e., accidents beyond the design basis), considerable research has been conducted domestically and abroad, in particular, after the TMI-2 accident. [6-8] Various strategies are under development to minimize the consequences of severe core damage, for example, by looking into the phenomenological advancement of radioactive material inside the containment using thermal hydraulic or source term analysis computer codes, such as MELCOR, or by investigating the possibility of using existing plant equipment innovatively. [9]

Accident management, particularly severe accident management, is a very complicated field requiring

interdisciplinary experts. Here again, the capability of computers is being used to develop accident management systems; a paramount example is Computerized Accident Management System under development at the OECD Halden Reactor Project. [7]

In the U.S.A., much research has been carried out to better understand the phenomena following a core-damage accident, and many insights have been obtained [10]. These insights, augmented by other analytical or deterministic knowledge, may somehow be integrated into the computerized operator aids.

The risk management discussed earlier is closely related to accident management, because the better the risk is managed, the greater will become the plant's capability to prevent or mitigate accidents.

4. Emergency Management

As indicated earlier, emergency management seeks to protect the public from suffering the effects of a potential or actual release of radioactive material from the site. Specifically, it means the analyses, decisions, and actions to:

1) Establish emergency planning zones
2) Determine principal exposure pathways
3) Establish evacuation routes
4) Notify local authorities of the incumbent situation
5) Interrupt exposure pathways

There is an overlap between emergency management and risk management. The insights from the level 3 PSA can be useful in the decision making related to emergency management.

5. Conclusions

The recent trends of safety management in nuclear industry have been briefly discussed, focussing on risk management and accident management. The trends follow the lessons learned at the TMI-2 accident of 1979, taking advantage of the great advances in computer and information technology since then. Human factors engineering is considered in the backfitting to operating plants, or from the early design phase in the case of next generation nuclear power plants. However, verification and validation of the computer-based systems still remains an issue.

References

1. R. DiSalvo, M. Leonard, M. Manahan, and J. Wreathall, Management of Severe Accidents, NUREG/CR-4177, BMI-2123, May 1985.

2. P.K. Samanta, I.S. Kim, T. Mankamo, and W.E. Vesely, Handbook of Methods for Risk-Based Analyses of Technical Specifications, NUREG/CR-6141, BNL-NUREG-52398, December 1994.
3. I. Selin, PSAs---A Practical Assessment, International Conference on Probabilistic Safety Assessment Methodology and Applications, Seoul, Korea, November 26-30, 1995.
4. USNRC Policy Paper SECY-94-219, A Proposed Agency-wide Implementation Plan for Probabilistic Risk Assessment (PRA), memorandum from NRC Executive Director of Operations J. Taylor, Washington, DC (1994).
5. I.S. Kim, "Computerized Systems for On-Line Management of Failures: A State-of-the-Art Discussion of Alarm Systems and Diagnostic Systems Applied in the Nuclear Industry," *Reliability Engineering and System Safety*, **44** (1994) 279-295.
6. OECD Halden Reactor Project, Specialist Meeting on Operator Aids for Severe Accidents Management and Training, Halden, Norway, June 8-10, 1993.
7. OECD Halden Reactor Project, Specialist Meeting on Severe Accidents Management Implementation, Niantic, Connecticut, USA, June 12-14, 1995.
8. International Atomic Energy Agency, *Accident Management Programs in Nuclear Power Plants: A* Guidebook, Technical Reports Series No. 368, IAEA, Vienna, Austria, June 1994.
9. W.J. Luckas, J.J. Vandenkieboom, and J.R. Lehner, Assessment of Candidate Accident Management Strategies, NUREG/CR-5474, BNL-NUREG-52221, March 1990.
10. F. Eltawila, R.G. Fitzpatrick, J.R. Lehner, et al., Severe Accident Insights Report, NUREG/CR-5132, BNL-NUREG-52143, April 1988.