OVERVIEW OF PROBABILISTIC RISK ASSESSMENT METHODOLGY

Taesung Ha (PhD student)
Department of Engineering Physics, McMaster University, 1280 Main St. W.
Hamilton, Ontario, Canada L8S 4L7 hats@mcmaster.ca

ABSTRACT

Probabilistic risk assessment (PRA) has provided consistent methodology for systematic and quantitative safety studies in nuclear reactors. This method has been widely applied for reactor safety studies around the world, and was accepted as one of the major safety analysis tools in nuclear reactor and other complex engineering systems. General procedures for Level 1, 2 and 3 PRA analyses will be described and some of the important tasks in each level would be explained. The supplementary tasks of uncertainty and importance analyses will be discussed in general terms. The strengths and weaknesses inherent in current methodologies will be introduced.

1. Introduction

Nuclear reactor safety at its design stage or during its operation has been addressed in terms of defense-in-depth principle, which states installation of independent multiple barriers to prevent release of radioactive materials to the environment. This principle incorporates several safety features of redundancy and large safety margins. It proposed deterministic safety analysis with conservative assumptions and calculations, which devised design-basis accident (DBA) from practical considerations [1]. In DBA, most significant adverse accidents are chosen by experts, and the effectiveness of the barriers and safety systems in each accident is evaluated. Reactor safety is determined as a measure of the capability of withstanding those prescribed accident scenarios. If the reactor could mitigate the design-basis accidents, it can be considered that the reactor would handle any other accidents. To ensure reactor safety, a set of regulatory design and safety principle were implemented: redundancy of these safety-related system and continuous testing and maintenance, large safety margins, quality assurance in design and manufacture, etc. In general, one single safety system failure after initiating events was considered credible so that its consequence was estimated. However, some of the important events were excluded from any further analyses: multiple safety system failures after initiating events, common-cause failures, human errors, etc. Some of the reactor design flaws, any risks during reactor operation, etc are not appropriately evaluated. Thus there was a need for better evaluation in order to incorporate these risks in a more systematic and integrated process.

Probabilistic risk assessment (PRA) is an integrated safety analysis methodology that incorporates various information about plant design, operational practices, operating history, component and system reliability, human performance, etc in as realistic matter as possible. The first complete reactor safety study using this PRA method (called Rasmussen report or WASH-1400) was published in 1975 [2], which studied reactor safety in two US nuclear power reactors: one boiling water reactor and one pressurized water reactor. Although it was severely criticized in some areas of human error handling, lack of reliability data, etc, one of the main insights confirmed the Three Mile Island (TMI)-2 accident. The study showed that small LOCA is more risk-significant than large LOCA, which was previously considered to be a major threat from the DBA. Also, some of operation evidence showed that common cause failures have occurred effectively. Because PRA can provide quantitative estimates of the risks associated with complex engineered systems in systematic ways, it has been applied for the reactor safety studies in numerous reactors around the world after the TMI-2 accident. It has been also employed in the safety studies for chemical process facilities, waste repositories, and space systems. In this paper, general characteristics of PRA methodology, potential applications of its result, and strengths and weaknesses

inherent in current methodology will be discussed in general terms to better understand current PRA methodology.

2. What is risk?

Since risk need to be assessed quantitatively in PRA, it must be defined appropriately. For a proper risk definition at a fundamental level that can be applied to practical tasks in PRA, three basic questions should be answered [3]; "What can go wrong?" "How likely is it that that will happen?" "If that happens, what are the consequences?" Thus risk is expressed quantitatively by constructing a form of triplet sets:

$$R = \{< S_i, l_i, X_i >\} \quad (1)$$

where, S_i represents a i[th] "scenario", l_i the frequency of that scenario, and X_i the measure of consequences of that scenario. The first question of "what can go wrong?" is answered in the form of a scenario, or a set of scenarios S_i; the scenario can be combination of events and/or conditions that could occur). The second question of "how likely is it?" is answered in terms of l_i, which combines the available evidence and the processing of that evidence to quantify the probability and the uncertainties involved in l_i for each scenario. The third question of "what are the consequences" can be answered in terms of X_i for each scenario by assessing the probable range of outcomes such as core damage and dose to the public. In the following sections, the answer to these three questions will be described in detail.

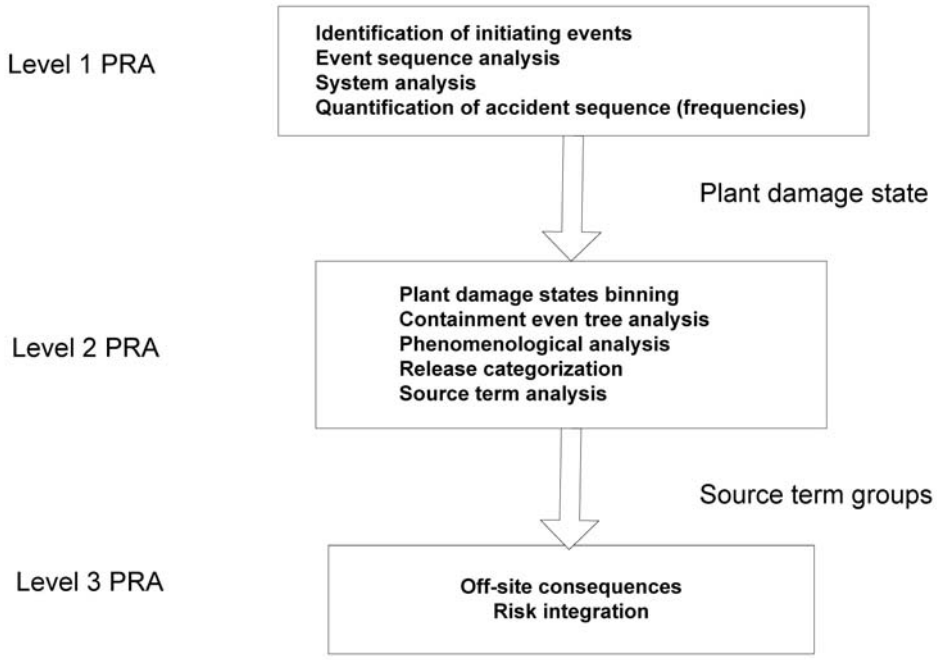

Figure 1 Three levels of PRA

3. PRA methodology structure

In order to analyze risk for nuclear power plants, PRA methodology was implemented to construct the risk triplet. For complete probabilistic analyses of reactor safety, analyses are generally divided into three levels or parts as shown in Figure 1:

- Level 1 evaluate and quantify the sequences of events that can lead to core damage or an undesired state of the plant.
- Level 2 evaluate and quantify the mechanisms, amounts, and probabilities of radioactive material release from containment corresponding to the core damage events.
- Level 3 evaluate and quantify the ultimate consequences to both the public and the environment from the core-melt events.

For risk quantification, two consequences are generally calculated: core damage frequency or off-site health effects. Level 1 PRA is conducted for core damage frequency quantification, whereas full three levels PRA is required for quantification of off-site health effect.

3.1 Level 1 PRA

In Level 1 PRA, the events that may challenge plant operation should be determined. The plant response to these events (accident sequences) is identified and its frequencies are quantified. Thus, risk is quantified in terms of CDF without further analysis of radioactive material behavior within containment and outside the containment. There are four major elements for Level 1 PRA.

- Identification of initiating events
- accident sequence modeling (event tree)
- System modeling analysis (fault tree)
- Quantification: data analysis, human reliability analysis (HRA), uncertainty analysis, and importance analysis

In order to conduct these tasks, plant familiarization task should be done first (probably by performing plant visit, preliminary plant analysis, etc.). The information related to the design and operation of the plant including procedures of emergency operation, test and maintenance, training materials, etc., must be obtained. These would provide necessary information for subsequent analyses.

3.1.1 Identification of initiating events

Postulated initiating events are the events that could result in core damage and hence a potential release of radioactive materials from reactor core, thereby challenging the safety limits of the plants. Their primary causes may be equipment failure, operator errors and human-induced or natural events, etc. There are several ways to identify initiating events. These include referring to previous initiating event lists, engineering judgment based on systematical review of the plant system and major components, and deductive analysis or operating experience in the plant under consideration. Some of the commonly analyzed initiating events are [4]:

- Internal events: loss of regulation and loss of reactivity control events, fuel power-cooling mismatch events, loss of coolant accidents, failures of safety support systems, and radioactive materials handling events, etc.
- External events: extreme meteorological conditions such as wind, lighting, precipitation or flooding, earthquake, external fires, and external explosions, etc.

3.1.2 Accident sequence modeling (event tree)

Possible accident sequences must be developed for each initiating event. These sequences delineate possible combinations of safety system/function successes and failures, which could result in either successful mitigation of the events, or undesired state of the plant: core melt or core uncovery. Hence, the

determination of success or failure criteria of safety systems is critical and requires a clear definition of core damage. The plant conditions corresponding to core damage states are usually defined in terms of core maximum fuel temperature, core exit coolant temperature, or coolant (or liquid) level below the top of the active fuel. Success criteria analyses would determine the minimum requirements needed for mitigating successfully the progression of an initiating event. The front-line safety systems for mitigating accident progression should be determined. Their supporting systems and functional relationships with other front-line safety systems should be identified. Then the success criteria for minimum equipment requirement is determined based on engineering mechanistic analyses: neutronic analyses, thermal-hydraulic analyses, etc. Typically, event sequences are modeled by event tree which depicts event sequences graphically. It arranges several safety systems identified in previous tasks in order of its heading and shows the relationship of safety functions to plant systems. The order of the headings shows information on the time sequence of functional interactions. Generally, event sequence diagrams are used to support event tree construction.

3.1.3 System modeling (fault tree)

In order to quantify event sequences, the unavailability of the safety systems appearing as headings (top events in system logic model) in event trees should be evaluated. Supporting system logic models are usually constructed for those safety systems. Thus event tree usually determines the boundary conditions for system modeling. There are several system modeling techniques such as fault trees, go charts, and reliability block diagrams. Among these techniques, fault tree analysis is usually selected in practical PRA studies. Fault tree represents the failure logic of a plant system graphically. It describes various combinations of the basic events that would lead to a predefined undesired state of a plant. Examples of those basic events can be component hardware failures, human errors, or hardware unavailability during maintenance or test, etc. The logic interrelations of basic events are usually developed to the level where reliability data are available; it could be system-level or component-level. The dependencies among these basic events should be analyzed with great care; functional dependencies on shared functions or on a process coupling, physical dependencies and human-interaction dependencies. To construct fault trees, it is very important to understand system operation, the operation of the system component, and the effect of component failure on system success. This information could be obtained through the procedures of the normal and emergency operation of the system, such as system operating instructions, maintenance procedures, and emergency operating procedures.

3.1.4 Quantification

To quantify the frequencies of accident sequences identified in event trees and its associated uncertainties, several tasks are followed: data analysis, human reliability analysis, and uncertainty analysis. Data analysis determines the frequencies of initiating events, hardware failure rates, and its maintenance and test unavailability. To estimate the unavailability of the basic events modeled in system fault trees, generic failure rates of components are usually obtained from a reference data bank. The data of plant-specific operating evidences (i.e., the information on component performance in response to a test or actual demand and component down-time during testing and maintenance) are obtained through operating logs, maintenance records, plant technical specification, and surveillance procedures. They are usually combined using Bayesian analysis to estimate the parameters of the probability distribution for unavailability of each basic event [5].

Human reliability analysis (HRA) is the special area that would identify, analyze, and quantify important human failure events (HFEs). They can be categorized into two types: pre-initiating and post-initiating HFEs. Pre-initiating HFEs are usually related to test and maintenance activities while post-initiating HFEs are the mitigating actions during accident progression. Thus post-initiating HFEs may include complicated dynamic interactions between operators and a plant system; thereby their analyses are

extremely complicated. Also they may pose direct impact on accident progression and are usually considered to be risk-significant. Several HRA methods have been developed to analyze HFEs such as the technique for human error rate prediction (THERP), success likelihood index method (SLIM), cognitive reliability and error reliability analysis method (CREAM), etc. Pre-initiating HFEs may be analyzed appropriately using the THERP, but post-initiating HFEs are difficult to analyze due to complicated dynamic nature during accident progression. In current PRAs, one of these HRA methods is practically implemented to quantify human error probability for the important operators' actions identified.

In PRA using event tree and fault tree analysis methods, Boolean expressions are generally used for quantification. They contain minimum cut-sets (MCSs), and the complete equations containing all basic events level for all accident sequences would be too large to be manipulated efficiently. From the fact that the top event frequencies are usually dominated by a few basic events and the contributions of many other basic events would be negligible, MCSs are usually determined through rare-event approximation by setting a certain truncation cutoff level. These MCSs would be of great significance for quantification since they may be mainly used to quantify the frequencies of all accident sequences and for their uncertainty analysis (see details in section 4). After the frequencies of initiating events are determined, the average annual frequencies of each accident sequence can be quantified using these MCSs with the unavailability of the top events from basic events (hardware failures, human failure events, etc.). MCSs are also used for importance analysis, which ranks the System, structure and components (SSCs) in terms of their contributions to the frequencies of accident sequences (see details in section 5).

The risk quantified from Level 1 PRA can be presented in various formats (table or pie diagram). Core damage frequency (CDF) mean and its associate uncertainty can be presented together. The consequent CDFs from different initiating events can be compared in terms of mean CDFs; pie diagrams can be useful. This comparison would be of great importance in terms of risk itself and its applications. That is, it would be used for financial allocation in risk management; more risk-important events could be financially prioritized.

3.2 Level 2 PRA

From Level 1 analysis, several accident sequences are identified and the frequencies of those sequences leading to subsequent core damage would be quantified. Core damage states can be categorized by their characteristics (e.g., plant status at the onset of core damage, etc). They are aggregated to plant damage states (PDSs) in several groups due to practical consideration (too many accident sequences are simply impossible to analyze by Level 2 PRA). These PDSs are served as initiating events and boundary conditions for Level 2 analyses. There are several tasks performed in Level 2 PRA [4]:

- Plant damage state categorization
- Containment event tree (CET) analysis; performance of containment systems in mitigating the radioactive material release to outside environment, and mode of containment failure
- Radioactive material release categorization
- Source term analysis

Plant damage states are served as the interface between system analyses (Level 1 PRA) and containment performance analyses (Level 2 PRA). They have a significant impact on the subsequent accident progression; they would set the boundary conditions for containment performance which are one of the barriers for radioactive release in defense-in-depth principle. Some of important PDS attributes [4] are listed in Table 1. This information is passed into the containment event tree analysis.

The information from the PDSs (see Table 1) can be used to determine the status of containment. To determine containment status, there are several simple questions asked (CET analysis); for example, if the

containment is bypassed or not isolated in terms of radionuclides. These questions are formed mainly on the PDSs or accident phenomena. Generally, an event sequence diagram method is used for containment event tree analysis. The resulting sets of event sequences form boundary conditions for phenomenological analysis of severe accident progression.

Table 1 Plant damage status attributes

Initiator type	• Large, intermediate, or small LOCA • Transients • Bypass events - Interfacing systems LOCA - Steam generator tube rupture
Status of containment at onset of core damage	• Isolated • Not isolated
Status of containment systems	• Sprays (if any) operate/fail or are available if demanded • Sprays operate in injection mode, but fail upon switchover to recirculation cooling
Electric power status	• Available • Not available
Status of reactor core cooling system	• Fails in injection mode • Fails in recirculation mode
Heat removal from steam generator	• Always operate/fails or are available if demanded • Not operating and not recoverable

CET analysis generates a large number of end states, some of which may be similar or identical. Thus these end states must be grouped to a small number of end states by utilizing release categories. For release categorization of radionuclides, several questions are asked again: timing and size of containment failure or bypass, operation of sprays, whether or not the core debris is flooded, whether or not the RCS is depressurized prior to vessel breach, whether or not vessel breach is prevented, etc.

Source term is referred to as the magnitude and composition of radioactive materials released to the environment and the associated energy content, time, release elevation, and duration of release. Its analysis includes the tracking of radioactive materials escaped out of the reactor core in the containment, reactor coolant system, and other building to the environment. It includes the processes of the retention of radioactive materials by natural processes through its paths. Simple parametric analysis is usually applied for source term analysis such as MECORE code, etc.

3.3 Level 3 PRA

Level 3 PRA includes two major parts of analyses: consequences analyses following various radioactive release (source terms) and risk integration of the results of Levels 1, 2, and 3 analyses. Source terms (or release fractions) serve as the input to Level 3 consequence analysis. Consequences are calculated in terms of [4]:

- Acute and chronic radiation doses from all pathways to the affected population around the plant
- Consequent health effects (such as early fatalities, early injuries, and latent cancer)
- Integrated population dos to some specified distance
- Containment of land from the deposited materials

One of these consequence measures is usually selected to integrate risk. From the results of all three PRA Levels, risk can be expressed in terms of its triplet sets by Equation (1). Note that the results of Level 2 and 3 analyses are conditional on Level 1 analysis. The final results can be summarized in table, or pie diagram, similarly to the CDF of Level 1 PRA results. Then they could be compared for different initiating events for applications such as financial allocation in risk management. Note that phenomenological uncertainties associated with Level 2 and 3 analyses are often of such a magnitude that they make the decision-making processes of risk-informed applications difficult.

4. Uncertainty analysis

The results of a PRA are to be applied in decision-making regarding changes in design or operating practices, economic decisions, or licensing purpose, so their significance must be interpreted in the light of uncertainties. Uncertainties are inevitably embedded in the risk quantified due to a lack of experimental data, lack of their precision, and lack of detailed understanding of the phenomena modeled; PRA studies deal with the occurrences of rare events. This leads to making several conservative assumptions, engineering judgment and subjective judgment for estimating the data unavailable to support PRA models. Ambiguous and unclear treatment of these sources would lead to controversies over the validity of PRA results. Hence uncertainty must be expressed using a mathematical language - probability theory.

Uncertainties are usually distinguished in recent PRAs as aleatory or epistemic uncertainty [6]. Aleatory (or stochastic) uncertainty arises due to physical variability (i.e., actual random behavior of system). It possesses a natural and unpredictable variation, and hence can hardly be reduced even if our knowledge about the system increases. In contrast, epistemic uncertainty arises due to a lack of the knowledge about system behavior and thereby could be eliminated from having complete information about the system. Generally, aleatory uncertainty is usually handled using probability distribution, whereas epistemic uncertainty is usually decomposed further into three distinct categories: parameter uncertainty, modeling uncertainty, and completeness uncertainty [7].

- Parameter uncertainties are related to imprecisions and inaccuracies in the parameters which are input to PRA models such as uncertainties in failure rates of the components, and some physical parameters for thermal-hydraulic codes.
- Modeling uncertainties are associated with uncertainties in the applicability and precision of the models used in PRA.
- Completeness uncertainties are uncertainties as to whether all the significant phenomena and all the significant relationships were considered in the PRA models.

In most PRA studies parameter uncertainties are quantified. Their sources are the uncertainties in the parameters in estimating initiating event frequencies, in failure rates and repair rates of component or system, human error probability, etc. Then an appropriate probability distribution for these parameters is selected; log-normal or gamma distribution is often assigned. The uncertainties are propagated through event sequences and system models (through event trees and fault trees). Monte Carlo simulation using appropriate sampling technique such as random sampling or Latin Hypercube sampling is usually conducted to quantify the overall uncertainties in the frequencies of accident sequences. In the approach where parameter uncertainties are analyzed, model structure is fixed. The effect of different models (modeling uncertainties) is generally investigated by sensitivity analysis where different models for human error probability (THERP, SLIM, etc) or common-cause failure analysis (Beta model or Multiple Greek Letter model, etc) may be used. In some cases, a more simple approach of quantifying modeling uncertainties can be applied by subjectively increasing certain failure rates and subjectively broadening the associated uncertainties. Completeness uncertainties are induced from whether or not all important accidents are included in PRA studies. It usually acts as a constraint and limitation on a PRA since the

PRA evaluates the risk from only the accident scenarios which can be identified and are considered risk-important.

In summary, in most practical approaches, aleatory uncertainty is treated using probability distribution functions and epistemic uncertainty is evaluated partially. Uncertainty analysis is generally performed about the uncertainties in parameters, whereas modeling uncertainties are evaluated in a limited way by using sensitivity analysis.

5. Importance analysis

In most PRA studies, importance analysis is supplemented, in which the Structure, System, and Components (SSCs) are ranked in terms of their contributions to the frequencies of accident sequences. Here "importance" is defined as the contribution of a component or cut-sets to the top-event occurrence. Its measures are evaluated from minimal cut-sets equations, which are defined as smallest combinations of basic events which lead to the top event occurrence if they all occur. The frequencies of accident sequences are also calculated from minimal cut-sets equations. The most commonly used importance measures are defined in the following equations [8].

$$FV = \frac{R_0 - R_i^-}{R_0} = 1 - \frac{R_i^-}{R_0} \qquad RRW = \frac{R_0}{R_i^-} \qquad RAW = \frac{R_i^+}{R_0} \qquad B = R_i^+ - R_i^-$$

where $R_i^+ =$ overall model risk with probability of basic event i set to 1, $R_i^- =$ overall model risk with probability of basic event i set to 0, and $R_0 =$ base reference case overall model risk. The Fussell-Vesely (FV) importance is a measure of the fractional contribution of a basic event to the overall model risk when the basic event probability is changed from its base value to zero. The Risk Reduction Worth (RRW) is the ratio of a base case model risk to the risk with the probability of basic event i set equal to 0 (the event cannot occur or the equipment is completely reliable) to the base case model risk. Note that RRW can give the information on the maximum possible risk decrease for the improvement of the basic event involved. Thus it could be very useful to identify which of the SSCs should be improved to reduce risk most. The Risk Achievement Worth (RAW) is the ratio of the model risk with the probability of the basic event i set equal to 1 (i.e., the event occurred or the equipment is failed) to the base case model risk. Birnbaum Importance (B) is difference in the overall model risks between with probability of basic event i set to 1 and with probability of basic event i set to 0. Thus it is completely dependent on the structure of system model and is independent of the current probability of basic event.

These importance measures can be applied in various areas: a model review and debugging effort, or risk-informed decision-making and regulation. For a model and debugging effort [4], events at the top or at the bottom of the table lists can be questioned; why are these events ranked high or low? If the answer is not reasonable or obvious, then the model should be rechecked. Any unexpectedness on the importance ranking may be indications of modeling error. They could be used in various risk-informed applications [9], and this discussion would be described in the section 6 in more details.

There are also several limitations of importance measures [10]. For instance, failure modes that are not modeled in PRA cannot be included in importance analysis. Importance measures are evaluated conditionally in that all other model parameters are essentially nominal for any given model parameter. Since the minimal cut-sets are determined from truncated models, corresponding importance measures are also limited. They are evaluated at the extrema (0, 1) of the defined range of probability and the credible (uncertainty) range for the basic event probability was not accounted for. Hence several approaches have been proposed to include uncertainties in importance measures. When one uses the information contained in importance measures, one should be aware of these inherent shortcomings.

6. Strength in current PRA

Most of the relevant information on plant design, operational practice, operational history, reliability of system and components, human performance, etc are incorporated into PRA and ranked in terms of their importance. This integrated approach is different from conventional deterministic approaches which are applied to individual issues, individual systems, etc. Thus PRA could be very beneficial in risk-informed applications in the fields explained below, since its results include comprehensive information of the plant under investigation. Also, they could be used for a communication tool; their analysts and users could express their opinion in specific technical terms and debating issues in PRA results.

PRA can produce valuable information on the plants investigated. All the important accident sequences from all initiating events can be identified and ranked in terms of their risk contributions. The Structures, Systems, and Components (SSCs) in those sequences are ranked by integrated approach (importance analysis). The result of these rankings can provide valuable information in various applications. Since most PRA studies calculate importance measures by ranking accident sequences and the SSCs, importance measures could give the information on which accident sequences are risk-significant, or which components, procedures, human actions are risk-significant. These rankings could be essential for risk management and the wise allocation of resources in reactor operation. In order words, risk importance measures could be used in reactor safety and regulation applications such as risk-informed equipment configuration control, quality assurance requirement, test and maintenance rules, and reactor (re)design [9, 10]. For example, based on the rankings, risk-significant SSCs can be identified using FV and RAW importance measures, and their reliability can be improved by changing their test and maintenance activities. Technical specifications that specify limiting conditions for operation and surveillance requirement (which specify surveillance test intervals for many components) can be optimized. The assurance of quality for safety-related SSCs can be adequately maintained; current stringent quality assurance for non risk-significant SSCs can be relaxed and unnecessary operational cost could be reduced.

7. Limitations in PRA

There are several weaknesses present in current PRA methodology framework; issues of scope and modeling issues [11]. Low-power and shutdown modes of operation are substantially different from normal full-power operation. Most of the instruments for measuring important phenomenological quantities are designed to operate in the operating conditions of full power, and most of the automated safety systems are not in optimum service mode. Note that instrumentations can not provide accurate information on the states of the plant in accident sequences so that this would place heavy burdens on operations' diagnosis in addition to manual execution of safety systems since they are not supported by automation. These issues should be understood better than they are today.

There are also modeling needs such as human reliability assessment (HRA) or external event modeling (e.g., fire and flooding). HRA handles both pre-initiating and post-initiating human failure events. These are categorized into two types of error of omission (EOO) and error of commission (EOC); EOOs are associated with the failure to perform a system-required task, whereas EOCs with the incorrect performance of such a task or the performance of an extraneous task with the potential to lead to some system-defined failure. Pre-initiating human failures could be analyzed relatively appropriately by existing HRA methods such as THERP or SLIM-MAUD. However, the post-initiating human failure events during accident progression (especially EOCs) could not be analyzed appropriately although they were considered to be substantially risk-significant; EOCs could be refereed to as any inappropriate actions that could aggregate accident scenarios. The dynamic interactions between plant and its operators during accident progression are too complicated to analyze adequately. The EOC opportunities during accident progression are generally so numerous that they could generate an unmanageable number of

accident sequences. Even their mechanism is not even well-understood yet. This issue of EOCs has been a central issue in HRA methods since 1990s, hence several methods being developed: ATHEANA, MERMOS, CESA, and CREAM. It is generally agreed that human errors are strongly dependent on surrounding context (so called error-forcing context). This implies that human error should be understood in its general context where it occurs such as performance shaping factors and management and organizational factors. This concept has been used in modeling of EOC mechanism, which is still under development. However, there are also other issues of the data validity of the human error rates and the dependencies analysis among various human performances during accident progression. Although there are several generic databases for human error probability such as THERP, more complete validity analysis should be provided in addition to EOC probabilities. The proper mathematical framework for the dependencies among various human failure events during accident progression is not formulated yet.

8. Conclusion

The general PRA method was discussed in general terms. Its procedures in all three levels are briefly described as well as the presentation scheme of the PRA results. Theoretical concepts of the important additional tasks of uncertainty and importance analyses are also presented. The applications of the PRA results are illustrated in risk-informed application and as a communication tool. The strengths provided by the PRA method should be maximized by considering carefully its inherent weaknesses. Even though PRA could provide a very powerful and consistent methodology for systematic and quantitative safety studies in nuclear reactors, PRA should be implemented complementary with DBA for reactor safety study due to its inherent weakness. Some of these weaknesses have been investigated extensively and improved greatly over the past decade but more rigorous investigation on some critical issues should be furthermore extended.

9. Reference

1. W. Keller, and M. Modarres, “A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen”, *Reliability Engineering and System Design* 89 (2005), 271-285.
2. USNRC, “Reactor safety study-an assessment of accident risks in U.S. commercial nuclear reactors”, *WASH-1400 (NUREG-75/014)*, 1975.
3. S. Kaplan and B. J. Garrick, “On the quantitative definition of risk”, *Risk analysis*, vol 1, No. 1, 1981.
4. USNRC, “Kalinin VVER-1000 Nuclear Power Station Unit 1 PRA: procedure guides for a probabilistic risk assessment”, *NUREG/CR-6572, Rev. 1*, 2005.
5. G. Apostolakis, “Data analysis in risk assessment”, *Nuclear Engineering and Design*, 71 (1983), 375-381.
6. S. C. Hora, “Aleatory and epistemic uncertainty in probabilistic elicitation with an example from hazardous waste management”, *Reliability Engineering and System Design* 54, 217-223, 1996.
7. W.E. Vesely and D.M. Rasmuson, “Uncertainties in nuclear probabilistic risk analyses”, *Risk analysis*, Vol. 4 (4), 313-322, 1984.
8. M.C. Cheok, G.W. Parry, and R.R. Sherry, “Use of importance measures in risk-informed regulatory applications”, *Reliability Engineering and System Design* 60 (1998), 213-226.
9. I.B. Wall, J.J Haugh, and D.H. Worlege, “Recent applications of PSA for managing nuclear plant safety,” *Progress in Nuclear Energy*, Vol. 39, No. 3-4, 367-425, 2001.
10. M. Borst and H. Schoonakker, “An overview of PSA importance measures”, *Reliability Engineering and System Design* 73 (2001), 241-245
11. G. Apostolakis, “On PRA”, *Nuclear News*, March 2000.