Understanding PRA from Perspectives of History, Technology, and Culture

Xiangcheng Kong, Chunrui Deng

Science and Technology on Reactor System Design Technology Laboratory, Chengdu, 610041, China. tony.xkong@163.com

ABSTRACT: *In review of the PRA's history, technology, and culture, insights are presented on risk communication, closed-loop management, and iterations of analysis. PRA is a practical technology used in the safety management, so communications are very important for the PRA professionals. The safety level of a nuclear power plant could not be improved by only risk insights, the PRA approach should be applied in a closed-loop management system. The success oriented deterministic analysis and the failure oriented risk assessments are complementary and iterative with each other, the iterations of the two kinds of analysis will be very important.*
KEY WORDS: *Failure Oriented, Closed-Loop, Iteration*

0. INTRODUCTION

By review of the probabilistic risk assessment (PRA) history in the America, analysis of the PRA technology, and discussions of the culture background of PRA application, this paper deepens the understanding of the PRA approach and its function in risk assessment and risk management. Each of the next three sections will focus on one of the topics of history, technology, and culture respectively, with other topics involved as well.

Human binary way of thinking could be easily explained as "one divides into two". Facing risk, on one hand, we hope safety and no bad things happened, and we expect the successes of the prevention and mitigation. On the other hand, we consider the possible bad consequences and their likelihood, and we evaluate the failures of the prevention and mitigation. Fig.1 is Tai Chi Graph, and it is used to explain the two ways of thinking. The left side is success oriented and the right failure oriented; white means success and certainty, black failure and uncertainty.

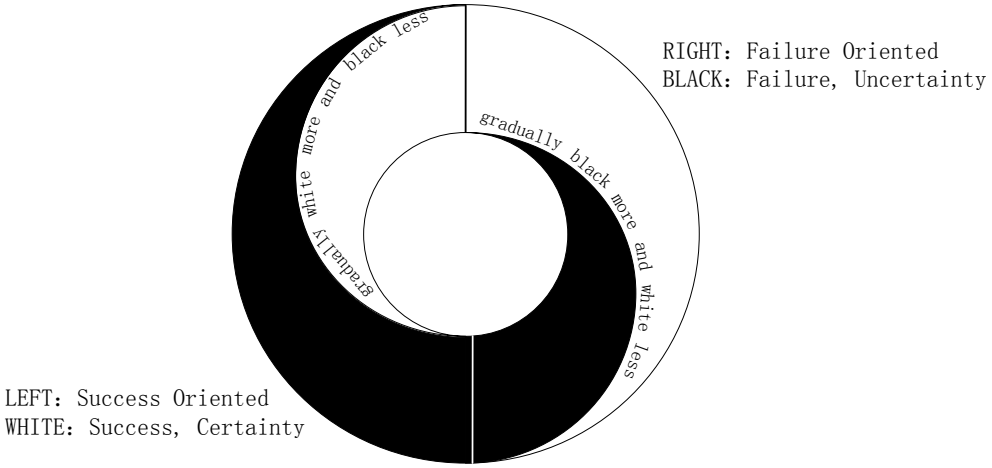

Fig. 1. Description of the two way of thinking with Tai Chi Graph

For nuclear facility, success oriented safety analysis means to consider potential accidents, then design engineered safety features (ESF) to successfully mitigate the presumed accidents, finally prevent large release consequences and guarantee safety. The defense-in-depth philosophy originated as a military strategy to delay the advance of the opponent by relying on multiple layered lines of defense instead of a single strong defensive line[1]. Another viewpoint showed that Du Pont engineers' reactor design framework of independent, functional and structural sub-systems brought out the defense-in-depth concept for nuclear safety[2]. Along with the accident progression, the multiple layers act as the gradually more successful defense, and are supposed to guarantee the successful accident mitigation.

Failure oriented risk assessments, on the contrary, addresses on failures and the possible consequences resulted from failures. Along with the accident progression, all the possible failures must be considered, including system, structure, component (SSC), initiating events, human error, etc., and gradually more and more failures are introduced. The basic philosophy of PRA could be summarized by three questions: What can go wrong? How likely is it? What are the consequences?

People's binary thinking way exists since civilization. The two thinking ways are mutual complementary, iterative, and not conflictive. For the purpose of safety, the knowledge, experience, and technology have been accumulated, developed, and innovated, but the fundamental philosophy have not varied significantly, being aware of these and hereby observe the history.

1. HISTORY

History of PRA is reviewed and insight is presented along with the history description. The history is divided to two phases, heading with the starting landmark event WASH1400 and GL88-20.

1.1. WASH-1400

In America, the early engineering test reactors were built in remote areas, in 1950, the WASH-3 report described the thumb rule for sitting, which was the earliest failure oriented risk assessment. The exclusion distance was directly determined by the reactor thermal power. Without containment, after an uncontrolled release of radionuclides, outside the exclusion area, the calculated radiation exposure should be less than the lethal dose threshold.

For the civil nuclear industry, the earliest risk assessment was the WASH-740 report, "*Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants*". The original impetus for non-military applications of nuclear energy in America was influenced by political factors, not because of the requirements for electrical power. An indemnity legislation for nuclear reactor accidents, which was included in the Price-Anderson Act, was regarded as necessary by the Joint Committee on Atomic Energy (JCAE), Atomic Energy Commission (AEC), and the nuclear industry. The WASH-740 report was a supporting technical input for the indemnity provisions of the Price-Anderson Act. Under the shadow of cold war, truths were not clear: Considering those political factors, how supportive was the Price-Anderson Act for the initiation of civil nuclear industry? Comparing state interest with public safety, was risk assessment concerned with emphasis?

More attention was paid to the success oriented analysis until the TMI-2 accident. In 1960's, facing increasing number of plant applications, AEC began to establish a general design criteria. The Appendix A of 10 CFR 50 came into being in 1971; section 50.46 and Appendix K defined the final criteria for the Emergency Core Cooling System (ECCS), including the five acceptance criteria for ultimate accident. At that time large loss of coolant accident (LOCA) was mainly considered as ultimate accident. The traditional deterministic safety analysis is arranged in the Safety Analysis Report Chapter 15 (Ref. 3), which is typically considered as Design Basis Accident (DBA) approach. For DBA, conservative methods and assumptions must be used, single failure rule must be considered, and finally the acceptance rules must be satisfied.

Two papers[4/5] in 1960's enlightened the idea for PRA methodology. F.R. Farmer used the effect of iodine-131 to represent consequence, and the famous Farmer Curves was presented as limit criteria for acceptable risk, comprehensively considering the consequence and frequency. The concept breakthrough leaded to a new era of risk evaluation, using the integration of consequence and frequency to measure risk. Some people consider Farmer and his staff as the originator of PRA.

The WASH-1400 report was regarded as the first complete PRA report addressing the nuclear power plant (NPP). In 1972, Senator John O. Pastore, then the Chairman of the JCAE, helped initiate the Reactor Safety Study (RSS) project, Professor Norman Rasmussen and his group started the study and finished the project in about three years, so WASH-1400 report is also known as Rasmussen report. This report performed quantification analysis for the radioactivity consequences and the frequency of the consequences. Comparing with the traditional deterministic safety analysis, other advances are: comprehensively considering all the initiating events, human errors, SSCs, etc, identification of all the possible accident sequences leading to radioactivity release.

No conflictions exist between the failure oriented risk assessment and the success oriented safety analysis, moreover, they are mutual complementary. The new PRA approach presented in 1974 showed consistency with the defense-in-depth philosophy, the consequence addressed in Level I PRA is the failure of the first layer defense, i.e. the first fission product barrier – fuel cladding; and the consequence in Level II PRA is the failure of the third fission product barrier – containment. However, people did not like the report very much at that time. Lewis Committee, who worked as the review group for the RSS project, commended the innovative method and found several good qualities, with many issues poorly handled. At that time Nuclear Regulatory Commission (NRC) staff was more familiar with the deterministic safety analysis and accepted the Lewis report as criticism.

As cultural phenomena, people like the success oriented analysis, one reason is the analysis "guarantee" success, and the other reason is that the failure oriented risk assessment sounds just like a bad omen when nothing can do to avoid the failures. At the very beginning NRC did not realize how to use the quantification results and the risk insight presented by WASH-1400 report. The RSS study was originally proposed by the higher level of management, not AEC or NRC, the one who demanded the risk assessment at the beginning was JCAE.

In the field of nuclear safety, it was reasonable for the deterministic analysis came into being first and the PRA followed. In 1950's and 1960's, when the large nuclear power plants were firstly designed and the radiation safety was considered, there were no design experiences, no design criteria, no knowledge of accident, no operator or plant staff, etc. So presuming some "credible" accidents and designing ESF to mitigate the accidents, to guarantee the mitigation success, the success oriented thinking was correct and reasonable. On the other hand, with the accumulation of knowledge level, operation experience, accident experience, experiment data, etc, for the operating NPPs, the PRA assessment was necessary to identify all the possible accident sequences, to evaluate the potential radioactivity consequences, and to quantify the probability. The WASH-740 had no concrete research object, so it makes no sense to compare its conclusion with the WASH-1400 conclusion for Surry and Peach Bottom NPP.

In 1979, accident happened at the three miles island (TMI-2) plant. Before the TMI-2 accident the deterministic safety analysis dominated the accident analysis, but the TMI-2 accident went beyond DBA, the real accident scenario did not obey the single failure rule. The scenario was a series of induced accidents: loss of feed water, small LCOA because of the stuck open of PORV, loss of ECCS because of human error. Generally speaking, the TMI-2 accident proved that the PRA method is necessary.

Before the TMI-2 accident, NRC and the nuclear industry believe the credible DBA, and the safety analysis focused on large LOCA, especially the double-end guillotine break as the ultimate accident. The logic was: analyzed with conservative method and assumption, deterministic conclusion could be drawn that the most severe ultimate accident could be "successfully" mitigated, then realistically happened accident could be "bounded" by the conservatism, and the less severe accident would also not progress to core damage. For a success oriented analysis, the verification of the successful mitigation is the purpose of the analysis.

The success oriented deterministic analysis neglected human error, combined or induced accidents, SSC failures more than single failure rule, etc. As failure oriented method, no need to aim at successful mitigation, no requirement for the conservative bounding, WASH-1400 addressed and emphasized on small LOCA, human error, induced accidents, all possible SSC failures, etc. WASH-1400 pointed out the potential risks from human error, concluded small LOCA is the largest risk contributor, and identified an accident sequence similar the TMI-2. So the failure oriented risk assessment is a necessary complement to the success oriented safety analysis, as shown in Fig.1, make it a complete circle.

In the early 1980's, plants at Zion, Indian Point (Units 2/3), Seabrook, Oconee developed PRA analysis. In 1983, the PRA procedures guide, NUREG/CR-2300, was finished. The draft of NUREG-1150 "*Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*" was issued in 1987 for public comment. These were the prelude of GL88-20.

1.2. GL88-20

NRC was not clear about how to use the PRA tool when WASH-1400 was born in 1974. The president commission responsible to investigate the TMI-2 accident suggested that the WASH-1400 report might be an approach to solve the problem. To execute the problem solving, large amount of preparation work had to be done. In 1988, NRC was well prepared and ready to use the PRA tool, then they issued the #20 Generic Letter (GL), Individual Plant Examination for Severe Accident Vulnerabilities (IPE).

As cultural phenomena, examinations are the most important means of national nuclear safety supervision, and often promote the nuclear safety regulations to a higher level. For example, after the Fukushima accident in 2011, nuclear safety examinations were executed all around the world and resulted in more strict regulations afterwards in many countries.

The PRA tool was suggested to be used for the examination, and this was the beginning that PRA was used in closed-loop plant safety management. The word "closed-loop" means to find problems and solve problems; there must be a feed back to the initial risk insight so that the management loop could be closed. The feedback could be directly a problem resolution, such as the SSC hardware improvement or operation procedure revising update, or just risk informed decision making (RIDM). Fig.2 shows a closed-loop management flow chart from PRA to improvement. Anyway, the PRA is just a tool for vulnerability identification, is just one part of the closed-loop risk management. The safety level could not be improved depending only on PRA.

The closed-loop concept depends on the perspectives or the view points. From the point of JCAE's view, RSS study and WASH-1400 report were also in a "closed-loop", since JCAE was responsible to control the founding for civil nuclear development, JCAE should make high level decision on national energy strategy facing the anti nuclear activist, and one of the purposes of RSS is to support the further modification of Price-Anderson Act. In this paper, the point of view is limited

from the NPP or NRC. Originally the WASH-1400 report was not developed for vulnerability examination, so it was an open-loop risk assessment at that time for NPP or NRC.

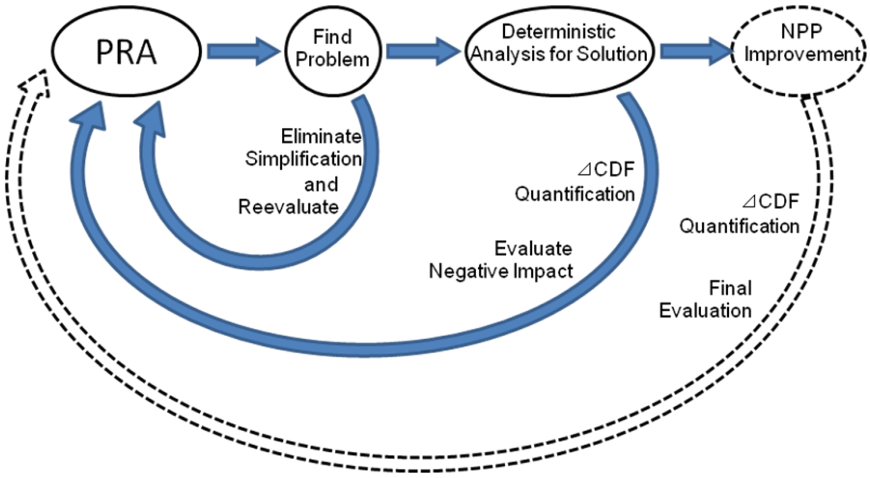

Fig. 2. Closed-Loop Management Flow Chart

The word open-loop is not supposed to be linked with derogatory sense. It is necessary to make it clear that the one tool of PRA was (is or will be) used for many different purposes, in past, at present, and in future. These two words are defined for convenience in this paper. For NPPs, the PRA is used for closed-loop safety management. PRA is also used for insurance, national energy strategy, or public risk communication, but these applications are open-loop for NPPs. NRC might use PRA for both open-loop and closed-loop purposes since they are supervising NPPs and facing public, congress, etc.

An example of open-loop application was the famous question "how safe is safe enough" answered with PRA method. In 1983, NRC approved two qualitative safety goals and two quantitative objectives (0.1%) determining the achievement of the qualitative goals. From 1986 to 1990, the two "0.1%" were transformed to overall CDF<1E-04/r-y and LRF<1E-05/r-y. However, in closed-loop PRA application, question "how safe is safe enough" will not be concerned primarily for the safety management, and the key points are no longer the overall core damage frequency (CDF) or large release frequency (LRF). The emphases were changed to be plant vulnerabilities, dominant CDF contributor of SSC, dominant accident sequences, the variation of CDF, etc.

In the 1st section of summary, the GL88-20 stated four general examination purposes. Considering the PRA closed-loop application, the four purposes could be rewritten as following:

- Find problems with PRA method, i.e., plant vulnerability identification, including:
  1. appreciation of severe accident behavior, this is the basis for deterministic part of Level II PRA;
  2. Identification of the severe accident sequences, this is the deterministic part of Level I PRA;
  3. Quantification of CDF and LRF, this is the statistical part of PRA;
- Try to solve the problems, i.e., reduce the overall probabilities of core damage and fission product releases by modifying hardware and procedures that would help prevent or mitigate severe accidents.

In the 2nd section of the GL88-20, NRC expected the utility's staff participating in the IPE to reach 6 goals, the first 3 goals were about the identification of problems, and the last 3 goals were about improvements. PRA was firstly mentioned as one of the three acceptable approaches in the 4th section "Methods of Examination". The four general purposes above are not the original words in the 1st section of GL88-20. Instead of a consolidated package of techniques as PRA, NRC hoped the industry or academy could present other approaches, which might be better. The prudence of NRC displayed an example for nuclear safety culture. The PRA consists of two parts: deterministic and statistical, and these will be discussed in the next Chapter of technology.

In the PRA history, WASH-1400 and GL88-20 (including NUREG-1150 and so on) were two landmark event leading the PRA technology development After the GL88-20 the examinations were carried out by the NPPs in America. For the power operation mode, all the plants used PRA method. In 1992, industry finished 74 PRA reports for the 102 units in America, CDF and LERF results were presented, PRA experiences and databases were accumulated, and it was ready for large scale PRA application. After 1992, gradually more PRA closed-loop application became dominant, and now, the word "PRA application" specifically means PRA closed-loop application.

In 1995, PRA had been well used in the nuclear industry, so the NRC timely published a policy statement on the use of PRA methods in all regulatory matters, and started the Risk Informed Regulations (RIR). Noted that the defense-in-depth policy would remain to be important and PRA was mainly used to reduce the unnecessary conservative regulatory requirements. In 1998, NRC issued Regulatory Guides RG 1.174-1.178 for the risk informed applications, including: General Guidance, In-service Testing, Technical Specifications, and In-Service Inspection. The concepts of safety margin and

defense-in-depth are still required in all these applications. Also in 1998, Reactor Oversight Process (ROP) was proposed. Later under the ROP framework NRC implemented many PRA applications.

The RIR promoted the PRA applications of NPPs in America, improved the safety level and benefited the NPPs economically. The capacity factor increased to about 90% at present from 50-60% in 1970's. Improvement involved in the scram numbers, failures of mitigation system, nuclear worker dose, etc. However, the low capacity factor at early time should not be attributed to only technical reasons, but also political factors.

Closed-loop regulation code system leaded to closed-loop application of PRA, GL88-20 is the initiation of this phase of history. GL88-20 had extensive and long term influence to the field of nuclear energy. Next year, SECY89-012 leaded to the development and implementation of Severe Accident Management Guidance (SAMG), SECY89-013 leaded to the establishment of Maintenance Rule (MR), and so on. In all these projects PRA technology was involved.

2. TECHNOLOGY

Three characteristics could be observed in the Tai Chi Graph in Fig.1: dichotomy, gradual conversion, and cyclical motion. These will also be used in understanding the PRA technology.

2.1. The Deterministic Part

The PRA is a failure oriented risk assessment. As mentioned in the four general purposes of GL88-20, it consists of a deterministic part and a statistical part. In the deterministic part, the core damage (CD) failure accident sequences are identified by thermal hydraulic analysis, then in the statistical part, all the probability and frequency are quantified so that the dominant risk contributor could be identified. In the deterministic part of PRA, the event tree model is used to simulate the accident progression.

In the event tree model, the continuous accident progression is discretized by a series of nodes (or called functional events). The purpose of discretization is to simplify the accident progression analysis so that the Boolean logic could be used in the probability calculations. At each node, the accident will progress to different branches, where success criteria are used to classify the accident progressing states at the node. In Level I PRA, the success criteria address the success/failure of the mitigation system function or operator's action. In Level II PRA node questions might be asked instead of success criteria since the nodes in Level II PRA addressing the complicated severe accident phenomena.

For the traditional deterministic thermal hydraulic analysis, only the acceptance criteria will be compared for the calculated end state, e.g. the 5 acceptance criteria in 10CFR50.46. In PRA, the acceptance criteria are transferred to a set of node success criteria basing on thermal hydraulic analysis.

2.2. Error Analysis

There are two types of errors: considering the factual failure as success, i.e. errors by optimism; or considering the factual success as failure, i.e. errors by conservatism. In the traditional deterministic safety analysis, conservative methods and conservative assumptions are required so that the errors by optimism could be eliminated. Mainly the purpose of the DBA analysis is to verify the capacity of the ECCS in successful accident mitigation. The conservative bounding logic is necessary for the success oriented analysis. As in Fig.3(a), the conservative criteria should bound the uncertainty distribution of capacity.

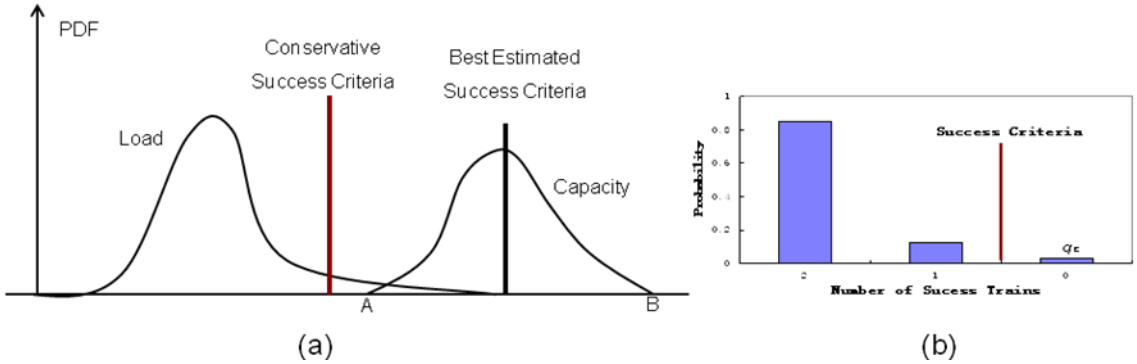

Fig. 3. The Determination of Success Criteria

Both conservative and best estimated assumptions are necessary for PRA deterministic part, as described in the Level I PSA guide by IAEA: About the Level 1 PSA, the overall aim should be to calculate a best estimate of the core damage

frequency while avoiding the introduction of excessive conservatisms wherever possible, since this may bias the results unnecessarily. Hence, the Level 1 PSA should be based on best estimate models, assumptions and data. However, some conservatism may be necessary where there is a high level of uncertainty, in order to avoid unjustifiable optimism[6].

As shown in Fig.3(a), when best estimated success criteria applied, errors by optimism could exist. Such errors are directly determination errors, which mislead the CD sequences into the OK sequences. Determination errors are not same as the two types of errors in Inference Statistics, which are the determinations of the point estimated value in or out the confidence interval. For both load and capacity, the uncertainty distributions are continuous in Fig.3(a), but often the distributions are discrete, as in Fig.3(b). For example, the capacity of one train of the safety injection system is sufficient to cover the load, i.e. the decay heat removal.

2.3. Iterative Deterministic Analysis

As the cyclical motion shown in Fig.1, the success oriented and failure oriented analysis could be iterative with each other. The new developed deterministic analysis includes probabilistic analysis such as BEPU and the PRA need more precise deterministic analysis. The errors by optimism in the deterministic part of PRA turned to be very important, especially for the extremely small number of CDF. For example, in the power operation internal events Level I PRA of AP1000 reactor, the total frequency for all initiating events is about 4/r-y, the overall CDF is about 2E-7/r-y. So for the OK sequences of the event tree, even the probability of the errors by optimism is assumed to be as low as one millionth, the CD frequency concealed in OK sequences would be much higher than that of CD sequences.

The discretization of the nodes makes it complicated to investigate if the large numbers of success criteria are conservative enough or excessively. Both continuous and discrete uncertainty distributions exist as the Fig.3(a) and 3(b), since the accident progressions are continuous and infinite possible progression end states should be considered. Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) has emerged as a new research field. One iterative scheme of probabilistic and deterministic calculations suggested continuous deterministic calculations according to a certain sample rule for the dominant PRA sequences[7].

Unlike the traditional deterministic analysis, which is performed with a strictly logical procedure and with conservative methods, the PRA's deterministic part exhibit many different format and content: in China, the thermal hydraulic calculations specifically addressing the success criteria (mainly the time window for operator) and arranged in Appendix D of PRA report; for the new reactor of AP1000 by Westinghouse, analysis in Appendix A addresses the OK sequences; in Europe for EPR reactor, the analysis for the design extension conditions are collected in SAR Ch 19. For those extremely small CDF results, the iterative deterministic analysis is necessary and the OK sequences must be verified with a strict, systematic and logical methodology as conservative as the traditional deterministic analysis, otherwise the extreme small numbers of CDF is meaningless. For example, the new passive systems must be verified by experiment with all possible uncertainties considered.

Best Estimation Plus Uncertainty (BEPU) analysis is one of the new deterministic analysis, in which probabilistic method is also used. The double 95% criteria are applied for the successful mitigation of the large LOCA accident. One 95% criterion is for the success probability, and the other 95% criterion is confidence level. BEPU is still considered as deterministic approach since it is a success oriented analysis. So the real classification for the variety of analyses or assessments is success oriented or failure oriented, actually probabilistic or deterministic methods could be used for anywhere necessary and reasonable. Not "*probabilistic*", but "*failure oriented*", is one of the essential characteristic of PRA.

Emphasis on "*integrated*" safety assessment might be unnecessary, while emphasis on investigation for real uncertainty distribution is insufficient. Last century in regard to BEPU, experiment researches addressing the parameter uncertainty of the large LOCA accident had been performed with large amount of funding in developed countries. However, as for PRA and some IDPSA approaches, the generation of uncertainty distributions are not so rigorous, some of them come from engineering judgments, or even just by assumptions.

2.4. Implicit Assumptions

For the purpose of best estimation of the CDF, the PRA cannot be performed with excessive conservatism. As a failure oriented method, the OK sequences in PRA event tree are not supposed to be the verification of successful mitigation. Besides the aleatory uncertainty sketchily shown in Fig.3, epistemic uncertainty also exists, so even conservative assumptions cannot guarantee the bounding of all uncertainties. Some implicit assumptions are used for the simplification of the event tree model, but according to such appreciation of accident phenomena some uncertainties would be neglected. Two of them are discussed in this paper: timing independence, simple linear system.

The factual accident phenomena happen along a time sequence, and recovery after SSC failure might happen at a later time. The simplified event tree model cannot fully consider timing of the node event and only a few important recoveries

such as diesel generator are addressed in PRA model. At present, the timing dependent PRA methods have been researched in the academic field.

The nuclear facility is considered as a linear system. Since the 1970's the theory of Chaos and Fractals have been developed. For non-linear systems, the error (or uncertainty) growth must be considered, e.g. butterfly effect. The Fig.1 is also called the primal chaos, with the gradual variation emphasized. In the PRA quantification analysis, the uncertainty propagation equally considers all the nodes in the event trees. However, for the early event on the upstream of the event tree, the uncertainty of the early accident state cannot be simply represented by the uncertainty distributions of the early events failure probabilities. The Lewis report also mentioned the problem of uncertainty propagation.

Modern view of defense-in-depth has a trend of balance: 'Defense in depth is achieved by a balance between measures to prevent accidents and systems to mitigate the consequences of accidents'[8]. How to understand the word "balance" depends on how to understand the "linear" system of nuclear facility. For a nonlinear system, definitely the early accident management is more important than the later defense. For a simple linear system as the uncertainty propagation assumed, even equal balance could be accepted. So the uncertainty propagation is basing on a assumption which simplifies the nuclear facility as a linear system. But the real accident phenomena could not be understood with assumptions and the risk insights might be misled. Actually the "balance" is just a trend: with accumulating knowledge on severe accident phenomena uncertainty, the severe accident mitigation could be addressed with more emphasis.

3. CULTURE

PRA is a practical technology used for the safety management of NPPs, and management involves the communications among people. The PRA's management application rooted in the cultural background, such as plant management, regulatory system, political framework, scientific research management, and so on. Hereby a few PRA related cultural phenomena are presented.

3.1. The Two Names of PRA/PSA

Before the first PRA forum in 1989 organized by American Nuclear Society (ANS), a new name, Probabilistic Safety Assessment (PSA), was suggested. So the two names of PRA/PSA appeared in the conference proceedings. Later in America, the name PSA was not accepted extensively, in the field of nuclear safety regulation and plant safety management, the name PRA was used more frequently. But in other countries, and in the IAEA documents, the name PSA is mostly used. Addressing the two names NRC issued a statement, indicating PRA/PSA are equal and interchangeable concepts.

In this paper, the "risk" and "safety" are understood as entirely opposite concepts. As in PRA, risk is measured by consequences and the potential frequency for consequences. So on the contrary, safety means no consequences for the plant states, e.g. the OK sequences after initiating events. Safety and risk compose all the possible states, or explained by probabilities, $P_{safety}+P_{risk}=1$. As a cultural phenomenon, some people understand the safety as "acceptable risk" by philosophical speculation, since absolutely zero risks are impossible in real life and people have to face risks. However, simple understanding is convenient for people's communication, and for engineering practice it is much easier to define the concepts as Fig.4(a), otherwise as Fig.4(b), the word "acceptable" need more definitions and the expression of "unacceptable risk" is inconvenient.

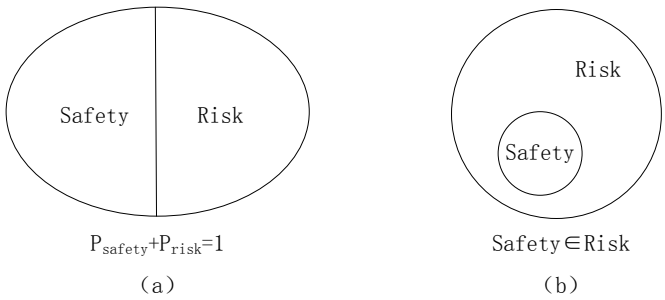

Fig. 4. The Concepts of Risk and Safety

As a cultural phenomenon, the name change is worth to note. In a social group, the thinking of each individual perspectively to some extent reflects the overall thinking of the group, in turn, the overall thinking inevitably impacts the individual thinking, and this is called "*culture influences*". For science and engineering, the naming of a new method is often just naturally to name the method with its main characteristics. If the words in the name are not representative for the essential characteristics of the method, then the name might mislead people's thinking and communications, or called as "*words without weight*".

In review of history, the approach was firstly named as PRA, trying to help people understand the essentials in the approach. The approach takes risk as research object, and basically it is a failure oriented method. The name PSA emphasizes the "*safety*" benefits of the method, whereas the name PRA highlights the "*risk*" aspect of the method. Under the history background before 1989, nuclear technology and the nuclear industry had struggled to communicate to the public the benefits of the technology. If you try to communicate the benefits of nuclear technology, and use "*risk*" methodology to prove the "*safety*" of the facility, your starting point is weaker. When the public hear the word "*risk assessment*", people will associate the technology with risk, but if the public hear the word "*safety assessment*", people will interpret it as a method that helps determine the degree of safety. This is a more positive statement and more reassuring to the public.

This approach has been used for a variety of purposes, as mentioned before, that are classified into two kinds: closed-loop and open-loop purposes. So considering the open loop purposes of public risk communication, the name PSA was suggested. But only the closed-loop PRA application could really help to improve the nuclear safety level. From the open-loop perspective, if only the equation "$P_{safety}+P_{risk}=1$" is agreed, then safety assessment is same as risk assessment and PSA equals to PRA. From the closed-loop perspective, it is the risk contributor or risk variations that be mainly concerned, not the overall safety level or risk level, so the name of PSA is not representative for the essentials of the approach in closed-loop applications.

In a society, interesting cultural phenomena would happen when the open-loop PSA application become dominant. For example, through popular media, a company advertised their 3rd generation advanced reactor that it is 100 times safer than the 2nd generation of reactors, since its CDF is very small at 1E-7 order. But the new reactor could not keep "*advanced*" all the time, since soon later another new reactor made a new number of extremely small CDF. Finally, PSA became a game of numbers, the fidelity of PSA was doubted, and number manipulations were concerned.

The advocators for the new name of PSA would not like to see such a paradox: the name PSA emphasized the "*safety*" benefits of the method, but people indulged themselves in using small numbers to prove "*safety*", and neglected the closed-loop applications which emphasized the "*risk*", finally the PSA realized little "*safety*" benefits. Considering the difference of cultural background, the advocators presented the name changing suggestions in America around 1989, but for other countries situations were different, especially the absences of a closed-loop regulation system or examinations such as GL88-20. In other countries, the name of PSA was easier to get accepted but the closed-loop applications of PSA could not be anticipated.

Will the public believe those extremely small numbers of CDF? Unlike the predictions such as weather forecast for which the factual result could be known soon later, the small frequency could not be directly verified as a prediction, so the PSA results could not be directly perceived by public. After the Fukushima accident the word "*unforeseeable*" has been frequently used for the explanation of accident. Often the post-accident explanations show a sharp contrast with the pre-accident predictions, so the public believe more in the real events than the small numbers. Perhaps the renamed PSA could take a positive guiding role for the public psychology, and a propitious name could give the public psychological comfort.

However, within the nuclear industry, no comfort is needed; on the contrary, we need more dangerous warnings for the risks. As mentioned before, the nuclear safety level could not be improved only depending on risk assessment. In the closed-loop management process, the problem finders must actively communicate with the problem solvers. The names function as designations in the communication, and they can subtly influence people's thinking. Facing supervisors, plant operators, deterministic safety analysis experts, maintenance staff, and professionals in other major, the PRA professionals need to bring out risk insights and warnings for the risks, and then plant supervisors or regulatory bodies accordingly initiate the improving actions or RIDM. So not psychological comfort but risk warnings is needed from PRA.

3.2. The Culture Difference

Same technology is applied differently in various countries because of the different culture background. In the US, the RIR and PRA applications are going well, while in other countries the applications of the technology are not as well as that in the US. Hereby four aspects of reasons are presented for the difference: history, technology, regulations, and industry.

For the nuclear energy history in the US, there was such a period with relaxation of the nuclear safety regulation. One reason was from the political factors, the other reason lied in the technology development. In the early years large redundant safety margins were set to cope with the unknown uncertainties. So later along with the increasing of knowledge level, some safety margins were released and the unnecessary conservatism was removed, during this process the PRA was used for identification and analysis. But other countries did not undergo such a history process, the advanced technology were directly introduced. So they do not have the requirements with PRA for regulation relaxation.

In the PRA technology, the best estimated assumptions are often used. The method does not emphasize on conservatism and not involve with the safety margin concepts, which could bound the uncertainties and support the deterministic conclusion. The PRA is a failure oriented evaluation, so conservatism and safety margin might bias the assessment. The PRA

is not a verification of success and often the accuracy of the PRA is not guaranteed. Therefore, it is hard for other regulatory bodies to apply such an approach, while the more strict regulations are always applied in other countries.

The NRC is a unique agency in the world. Comparing the capacities and responsibilities of the regulation, the regulatory bodies in other countries are far away behind to catch up. For one thing the other countries are far away — the NRC occupies the best resources in the country. Its technology support organization (TSO) includes seven national labs and some consultant companies, NRC and its TSO have the most of the elites, and they have the best resources for the nuclear energy technology. The agency's capability match the responsibility — when any incidents or accidents happened at any plants the NRC would be questioned and blamed firstly. But the regulatory bodies in other countries are different, sometimes they are not required to solve the difficult problems, since they could introduce the most strict regulation codes, from NRC or IAEA, and require the industry to have the capability. The difference of the regulation might be the main reason for the unrevealing PRA applications in other countries.

The PRA require a large and living database for the fidelity. The American nuclear industry is doing well on data. For small countries, only a few nuclear units exist; for developing countries, the operating history is not very long and only limited number of data have been collected. After the GL88-20, it also took the American industry and regulation a long time to implement the PRA applications. Now the industry in other countries has realized the benefits of PRA and they are catching up.

4. SUMMARY

In review of the PRA's history, technology, and culture, some insights are presented. The three key insights could be summarized as: communication, closed-loop, iteration.

PRA is a practical technology used in the safety management, so communications are very important for the PRA professionals. For regulatory bodies that have not the best technology resources, communications are especially important since they need coordinate or call for the other technology organizations.

The safety level of a nuclear power plant could not be improved by only risk insights, the PRA approach should be applied in a closed-loop management system. The open-loop applications might exist in future, but within the field of nuclear safety, the closed-loop applications must be emphasized.

The success oriented deterministic analysis and the failure oriented risk assessment are complementary and iterative with each other. The methodology for the iterations will be the interested research areas and the regulation codes might be modified in future basing the new methodologies.

The goal of this paper is to present some insights on the history, technology and culture of PRA, so that people could have a well understanding on PRA and the PRA application could be promoted in countries other than America. PRA is not a tool calculating extreme small numbers to show safety level, and PRA is not just used for economic benefits and regulation relaxation. As a failure oriented risk assessment, PRA is a necessary complement for the success oriented deterministic analysis. The safety level of NPP could be improved, not predicted, by PRA, only that PRA is used in a closed loop management system.

ACKNOWLEDGMENT

The authors are grateful to the PRA workshops under the U.S.-China Peaceful Uses of Nuclear Technology (PUNT) Agreement. The organizers, the Argonne National Lab and the Suzhou Nuclear Power Institute, have held 8 workshops since 2010. The knowledge and experience shared by the American professors and experts are very helpful.

REFERENCES

1. NUCLEAR REGULATORY COMMISSION, "Historical Review and Observations of Defense-in-Depth", NUREG/KM-0009, U.S.NRC, (2016).
2. W. KELLER, 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 & System Safety*, 89, 271-285, (2005).
3. NUCLEAR REGULATORY COMMISSION, "Standard Review Plan", NUREG-0800, Revision 3, U.S.NRC, (2012).
4. F. FARMER, "Reactor safety and siting: a proposed risk criterion", *Nuclear Safety*, 539–48. (1967).
5. C. STARR, "Social benefit versus technological risk", *Science*, 19: 1232–8. (1969).
6. IAEA, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants", IAEA Specific Safety Guide No. SSG-3, para 5.7, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, (2010).

7. X. KONG, C. DENG, etc., "PSA Conservatism Analysis and Quantification for the LOFW Accident", *Proceedings of 21st International Conference on Nuclear Engineering (ICONE21-15299)*, July 29- Aug 2nd, Chengdu, China, (2013).
8. NUCLEAR REGULATORY COMMISSION, "Perspectives on Reactor Safety", NUREG/CR-6042, Revision 2, U.S.NRC, (2002).