Probability and Fukushima Daiichi Nuclear Power Plant Catastrophe

M. Shinozuka
UCI Distinguished Professor,
Department of Civil and Environmental engineering, University of California, Irvine

SUMMARY:
This paper describes the root causes of the catastrophe that resulted from the failure to protect Fukushima Daiichi Nuclear Power Plant under combined impact of March 11, 2011, M= 9.0 Tohoku Earthquake and the powerful tsunami that followed. The root causes are examined from the PRA (Probabilistic Risk Assessment) point of view specifically focusing on the event tree analysis used in fundamental design decision making for construction of Fukushima Daiichi Nuclear Power Plant reactors. This paper identifies a number of pitfalls the event tree analysis did stumble into. The paper then proceeds to recommend that a damage mitigation strategy be implemented in order to avert these pitfalls to ensure the needed power plant resilience and sustainability under uncertain hazardous events.

Keywords:
Probabilistic Risk Assessment, Boiling Water Reactor, Event Tree, Damage Mitigation Strategy, Tsunami

1. INTRODUCTION

An unthinkable consequence resulted from March 11, 2011, M= 9.0 Tohoku Earthquake followed by a powerful tsunami that assaulted the northeastern shores of Honshu island of Japan. In addition to the unacceptable level of human and property losses as shown in Table 1 under the combined impact of ground shaking and tsunami, the failure to protect Fukushima Daiichi Nuclear Power Plant from these impacts made this disaster a catastrophe of global magnitude. In fact, in this case, the failure not only resulted in a severe level of disasters centered around the power plant location, but also brought a long duration of radioactive contamination over the global environment. This study examines from the view point of PRA (Probabilistic Risk Assessment), the event tree analysis procedure that helped make design decisions for BWR (Boiling Water Reactor) reactors at Fukushima Daiichi Nuclear Power Plant. Specifically, this study identifies some pitfalls in performing the event tree analysis and proposes that a damage mitigation strategy be implemented to avert these pitfalls in order to make nuclear reactors significantly more catastrophe-resilient if not catastrophe-free.

Table 1. Human, property and monetary losses

Death Toll	**15,405**
Missing	**8,095 (23,500)**
Injured	**5,365**
Houses damaged	**552,260**
Roads, bridges, railways damaged	**3,592**
Estimated monetary loss	**$300,000,000,000**

2. EVENT TREE ANALYSIS AND DAMAGE MITIGATION STRATEGY

The event tree analysis is generally quite useful in supporting fundamental design decisions for a complex and important structure consisting of multiple components each of which serving its unique sub task and in combination, they enable the structure to perform a specific task of socio-economic significance. Low probability but high risk nuclear power plant, particularly reactor buildings, typically represents such a structure that demand the design decisions aiming at a high level performance in resilience and sustainability under uncertain natural (such as earthquake) and manmade (particularly terrorist attack) hazard events. The event tree analysis can integrate the concept of PRA in order to rationally model the uncertainty problems arising from probabilistic characteristics associated not only with the hazard events but also with the response capability of each component to the hazard events. However, the past nuclear plant accidents including the Fukushima Daiichi catastrophe strongly suggest the need for a more aggressive damage mitigation strategy. The strategy includes the development of more substantial damage mitigation procedures that can rapidly detect, diagnose, and respond to early signs of any anomalous behaviour of the components to prevent core melt or at least lead the reactor to a cold shut down. It is noted that, depending on the type and vintage of the reactor, the catastrophe may result from different causes and through different processes. Even then, the damage mitigation strategy appropriately adjusted must be developed. In this respect, it is notable that a paper titled "A Proposed Backup for Emergency Heat Removal System for Nuclear Power Plants Using Mobile Pumps and Liquid Chilling Units" was published in 1991 by K.P. Cheung (Cheung 1991). The method is aggressive in that it directly works on the reactor core notwithstanding the possible difficulty to access. A power point presentation of updated version of this paper is also available (Cheung 2012). The spirit of these papers exactly matches with the concept of the damage mitigation strategy just mentioned and they serve as a good pilot study to promote the damage mitigation concept. As shown later, the impacts of damage mitigation procedures will be integrated into the augmented event tree analysis in order to systematically protect reactors from unthinkable damage events. Note that conventional event tree should be constructed out of expected hazardous events and analyzed independently of the aggressive damage mitigation procedures which form a first and most effective line of defence against often fatal unthinkable damage events to save the power plant from catastrophe. Also, by implementing the damage mitigation procedures independently of event tree analysis, all the pitfalls associated there with will be avoided.

Unfortunately, the concept of damage mitigation strategy is not firmly integrated into the safety evaluation of nuclear power plants. Actually, this lack of damage mitigation strategies creates serious pitfalls when the event tree analysis is applied to nuclear reactors. For the ease of explaining the nature of these pitfalls, a post-earthquake event tree for a simple hypothetical BWR type nuclear reactor model is developed in Figure 1 where there are three events (A, B, and C) to be considered. Success or failure associated with each event is indicated by two arrows at each of the 4 nodes; Horizontal to the right shows success and vertical downward failure. This system then produces 5 event sequences (S1,S2,…,S5) ending up with 5 consequences (end events) I, II, III, IV, and V as shown below. The occurrence probability of each sequence (or each end event) can be computed using probability values for success or failure at the constituent nodes. As mentioned earlier, this process of event tree analysis for design purposes encounters conceptual pitfalls without a well developed damage mitigation strategy. Following Figure 1, four most prominent pitfalls are listed.

S1 = ① – ② – ③ – [I]
S2 = ① – ② – ③ – [II]
S3 = ① – ② – ④ – [III]
S4 = ① – ② – ④ – [IV]
S5 = ① – [V]

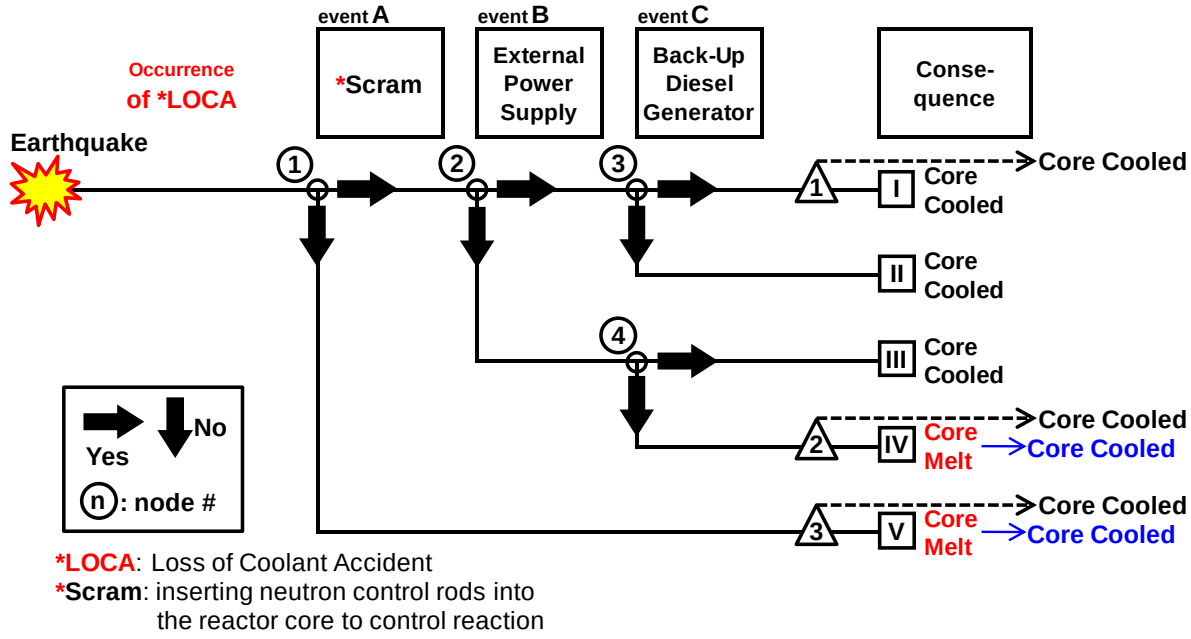


Figure 1. An Example of Simple Hypothetical Post Earthquake Event Tree

(1) The design was made to ensure that the probability of core melt event be extremely small. For this purpose, the occurrence probability values around once per million years or even smaller values were stipulated. This level of small probability values are statistically meaningless and misleading in engineering applications since it can be misconstrued to mean that the event will never occur. However, in estimating seismic resilience of an urban community in seismically active area where the small annual occurrence probabilities of the same extremely small range for scenario earthquakes of large magnitude are often used and integrated in the probabilistic resilience analysis without causing much controversy. This conceptual tolerance for the community analysis can be explained, in fundamental simplicity, by observing that in this case one can try to evaluate maximum level of the socio-economic losses arising from disastrous impact of the earthquake, whereas, in the case of nuclear catastrophe, no one can even guess the worst extent and complexity of the catastrophe.

(2) It is not possible to include all significant events or event sequences, particularly the latter in the event tree. For example, observing the Fukushima Daiichi Nuclear Power Plant catastrophe, consider the sequence of earthquake - tsunami wave - failure of diesel engine and generator which made ECCS (Emergency Core Cooling System) inoperable and eventually lead the reactor to core melts. This event sequence is recognizable in hindsight, but understandably, no one had a foresight to this specific sequence that is categorized as “unthinkable”.

(3) Even when a certain event is included, its impact can be underestimated. Fukushima Daiichi Nuclear Power Plant was designed for M 8.0 earthquake, while the actual Earthquake (3-11-2012 Tohoku Earthquake) was of M 9.0. Therefore, ground shaking intensity and tsunami wave height were both accordingly underestimated.

(4) Some end events (consequences) are “core melt” as shown in Figure 1. However all the end events should be “cold shutdown”.

More detailed nature of each of these pitfalls is described below.

Pitfall 1: Extremely Small Occurrence Probability

According to a transcript of Japanese parliamentary meeting (in 2010), a legislator questioned in essence, “Based on past experiences, both at home and abroad, we have to be prepared for worst-case

scenarios", and he further said. "We need to be ready for an extremely serious situation where the inability to eliminate the heat in the reactor after its shutdown could lead to melting of the reactor core." (This is exactly the scenario that happened at Fukushima Daiichi Nuclear Power Plant).
The director general of the government's Nuclear and Industrial Safety Agency, replied that such a situation was "theoretically possible" but "nearly unthinkable". This response was construed as saying that the event of question has zero occurrence probability. (Adapted from Wall Street Journal, March 28, 2011).

Pitfall 2: Unthinkable Event Syndrome
Charles Perrow in his book "*Normal Accident*" (Perrow 1999) declared "for high-risk technologies, no matter how effective conventional safety devices are, there is a form of accident that is inevitable". This is referred to as "unthinkable event syndrome (includes scenarios never thought about and scenarios thought about but not considered for the analysis)" in this paper. He further states that, "This is not a good news for systems that have high catastrophic potential, such as nuclear power plants, nuclear weapons systems, recombinant DNA production, or even ships carrying highly toxic or explosive cargoes. It suggests, for example, that the probability of a nuclear plant meltdown with dispersion of radioactive materials to the atmosphere is not one chance in a million years, but more like one chance in the next decade.
Jan Beyea wrote an article "*Second Thoughts*" (Beyea 1983) in a book "Nuclear Power: Both Sides", edited by Michio Kaku and Jennifer Trainer. In this article, focusing on nuclear reactors, Beyea discussed many issues of reactor safety concerns. It is particularly noteworthy that he did consider in 1983 that the core melt scenarios arising from the failure of Emergency Core Cooling System (ECCS), a very similar scenario that actually happened in Fukushima Daiichi Nuclear Power Plant. Also, Beyea had an amazing insight to the reactor safety and argued that "reactors are inherently flawed because safety devices were always added as an after thought, rather than being a fundamental consideration of the reactor design". This reminds us of disablement of Diesels and Generators, key components of ECCS, by tsunami in case of Fukushima Daiichi catastrophe. It would be interesting to see if Beyea's "after-thought" assertion applies to this case. If so, that may explain the rather casual level of

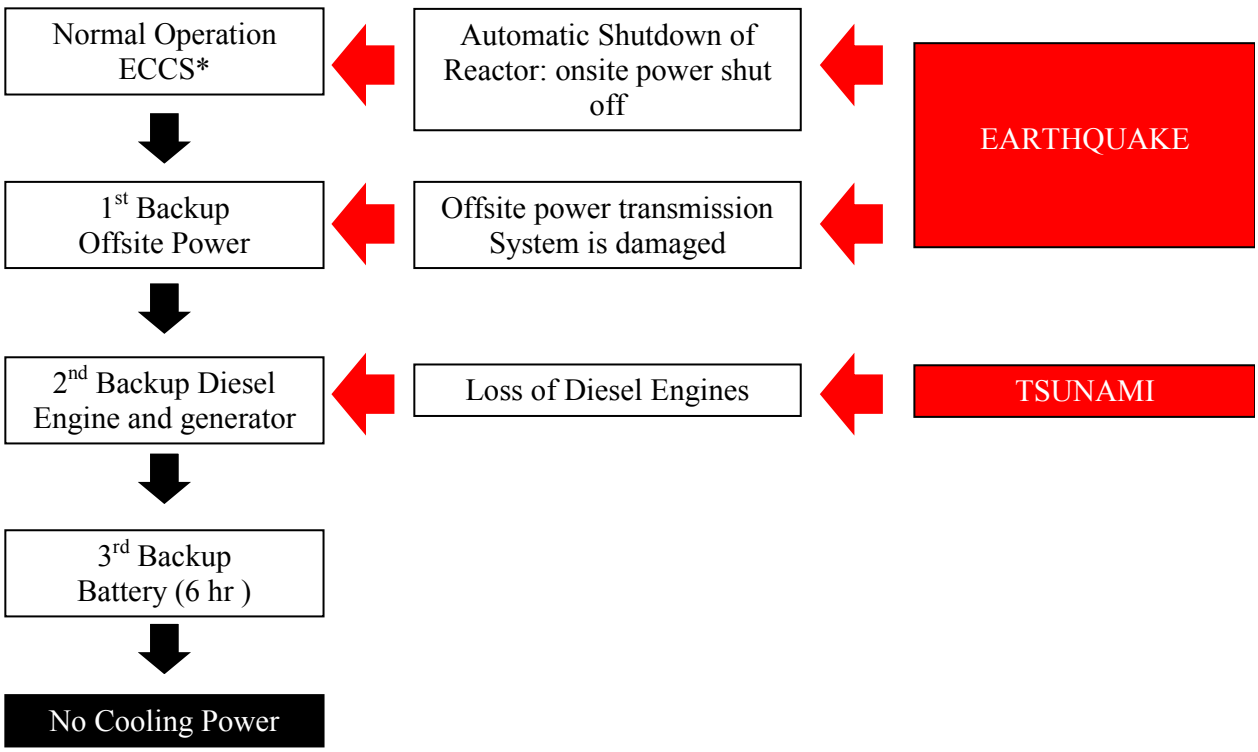
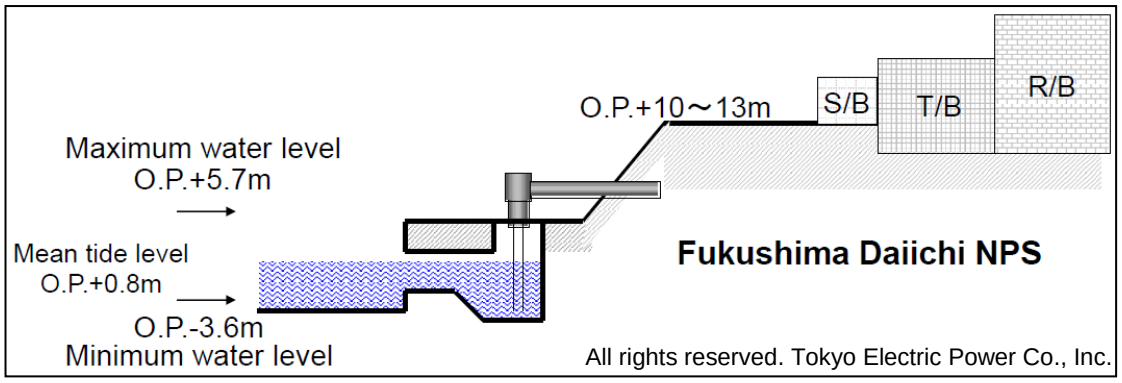


Figure 2. Process of ECCS Failure

protection provided for the ECCS components. They could have been installed in one of major buildings, or construct a simple but sturdy building to cover them.
In the case of Fukushima Daiichi Nuclear Power Plant, the accident was not inevitable in hindsight. It was due to low seismic reliability of offsite power transmission system, underestimation of earthquake magnitude and hence underestimation of resulting tsunami wave height, and lack of protection of ECCS system components. However, the total lack of the damage mitigation devices particularly those to prevent the core melt directly working on the core itself such as the cooling device proposed by K.P.Cheung (Cheung 2012) indicates an important strategic oversight notwithstanding the difficulty to access the core under these circumstances. At any rate, Perrow's prediction and Beyea's concern were justified. An unthinkable sequence of events did occur and reactors were led to core melt.
This sequence of unsuccessful attempt to backup the ECCS using conventional safety devices is described in Figure 2. The process was confirmed by NISA (NISA and JNES 2011) and it represents Perrow's "inevitable accident" and Beyea's "component added as an after thought". There is no information if the electro-mechanical components in the reactor buildings were damaged under the seismic shaking prior to the arrival of tsunami wave. If they were, the sequence of unsuccessful backup events could be quite different.

Pitfall 3: Under Estimation

For Fukushima Daiichi Nuclear Power Plant, tsunami effect was analyzed independent of the event tree format. In this analysis, the wave height of travelling tsunami was underestimated due to the underestimation of the seismic magnitude of Tohoku earthquake as 8.0 instead of actual 9.0. For magnitude 8.0, height of travelling tsunami wave is estimated 5.7 m.
Following Kawata (Kawata 2012*), and referring to Figure 3, the maximum height of the wave at the reactor building location is computed to be O.P. +8m indicating 8m above the official reference sea level at Onahama Port located approximately 60km south of Fukushima Daiichi Nuclear Power Plant. This value is obtained from Equations 1 and 2 upon amplifying by 40 % the height of the travelling tsunami wave with estimated wave height at O.P. +5.7m for M 8 earthquake as it crosses the tsunami barrier (see Figure 4). Observing Figure 3 and recognizing that this is below O.P. +10m (Equation 3) above which all the key structures including reactors are built or installed, it was concluded that the tsunami wave will not inundate the key facilities. However, the same analysis leads to a different conclusion for the magnitude 9 Tohoku earthquake for which the height of travelling tsunami wave was measured as O.P. +10m (Equation 4). Use of this value in the same model (Equations 4-6) leads to a conclusion that the tsunami wave height at the reactor location is O.P. +14m which is 4m above



Estimated maximum height of traveling tsunami wave (M 8.0 Design Earthquake)	= O.P. +5.7m	Equation 1
Amplified at the barrier by 40%*	= O.P. +8m	Equation 2
Location of Diesel Engine, Generator, Service, Turbine and Reactor Building	> O.P. +10m	Equation 3
Actual maximum height of traveling tsunami wave (M 9.0 Tohoku Earthquake)	= O.P. +10m*	Equation 4
Amplified at the barriers by 40%*	= O.P. +14m	Equation 5
Location of Diesel Engine, Generator, Service, Turbine and Reactor Building	< O.P. +14m	Equation 6

Diesel engines installed at O.P. +10m level (less than 14m) were impacted and inundated by tsunami* and lost functionality.

Figure 3. Elevation View

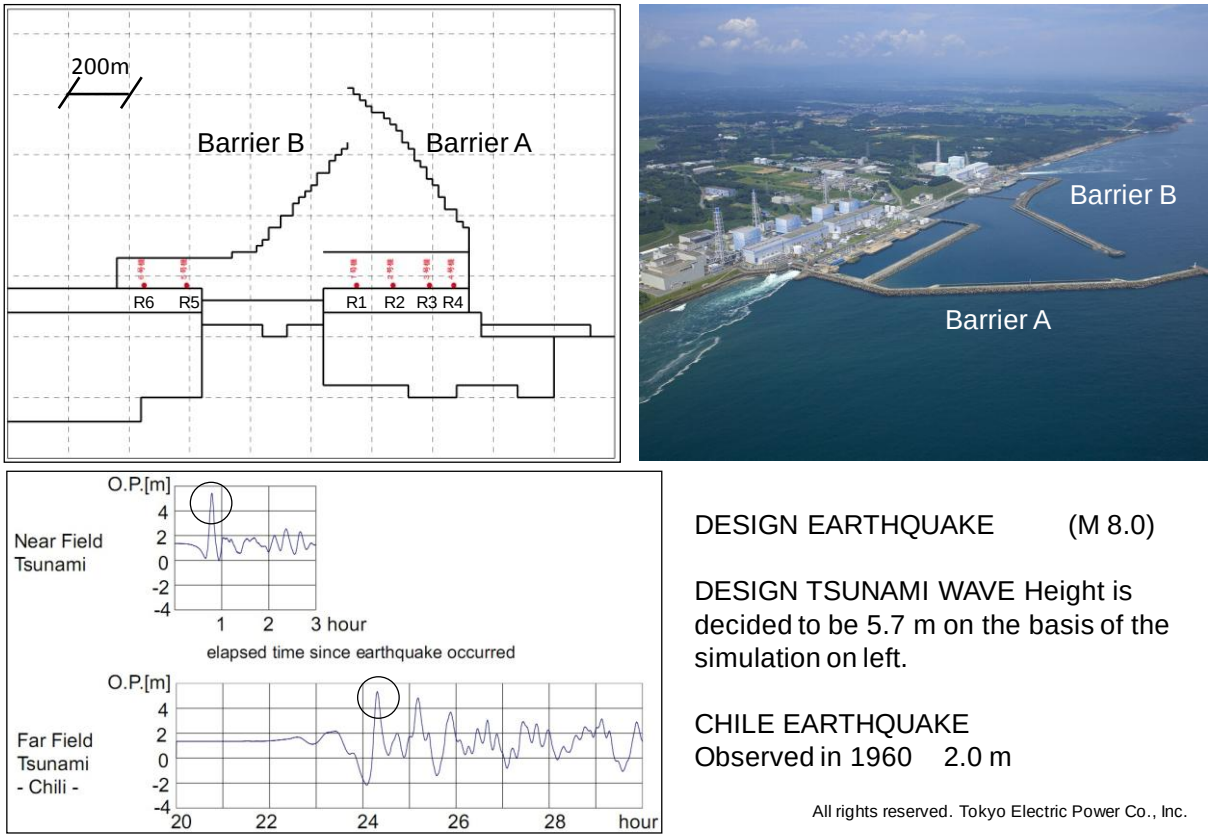


Figure 4. View of Barriers

O.P. +10m (Equation 3) demonstrating that the inundation results at the reactor location as actually observed. Furthermore, according to Kawata, tsunami wavelength and travelling speed are such that the inundation lasted as long as 4 hours.

Pitfall 4: Core Melt is End Event for Some Event Sequences

Some end events in the event tree developed for a model nuclear reactor (Figure 1) show "core melt". This is not acceptable. All the end events should be "core cooled". To achieve this, the damage mitigation procedure must be implemented. Triangle 1 in Figure 1 indicates a hypothetical scenario that a damage mitigation procedure is activated upon detecting severe system anomaly with a potential for core melt from unthinkable causes, although ECCS did perform well. Dashed line shows the procedure successfully brought the reactor core to the "core cooled" category. Triangle 2 also shows hypothetical initiation of a damage mitigation procedure. This time however recognizing the failure of ECCS system by monitoring the event sequence which suggests an imminent core melt at the end event IV. Dashed line indicates that the damage mitigation procedure successfully lead the reactor core to the state of "core cooled" category. Similarly, triangle 3 depicts a hypothetical scenario of a damage mitigation procedure being initiated upon recognizing the failure of the scram which will inevitably lead the reactor to a core melt condition at the end event V. The dashed line again shows the success of the mitigation procedure.

3. LESSONS LEARNED AND FUTURE RESEARCH

The event tree analysis is a useful tool to examine a specific risk event in terms of occurrence probability of that event often in combination with the associated loss appropriately measured. In case of Fukushima Daiichi Nuclear Power Plant, the core melt is undoubtedly the most important risk event, and every effort should have and must have been made to design the reactor system to ensure the probability of its occurrence to be extremely small. Nevertheless, the core melt did occur for various

root causes identified in hindsight. This lesson obviously will lead to improvement of design strategy for future reactors, retrofitting of existing BWR type and similar reactors. This however does not represent the key lesson. After all, there is a school of thought (Perrow 1999) that "no matter how effective conventional safely devices are, there is a form of accident that is inevitable". Also, there is a significant concern that "reactors are inherently flawed because safety devices were always added as an after thought, rather than being a fundamental consideration of the reactor design" expressed by Beyea (Beyea 1983).

The most glaring revelation is that the development of damage mitigation technology does not appear to have been enthusiastically pursued in recent years. However, if this technology delivered a well developed portable emergency cold reactor core shutdown device that is able to work directly on the reactor core as soon as the detection of the early sign of potential core melt, that represents a major breakthrough for upgrading reactor safety by significantly enhancing statistical confidence of PRA for the following means: Given a such emergency cold shutdown device to respond to a specific potential core melt scenario, the probability of success of this mitigation procedure can be evaluated conditional only to the state of the damage of the component of concern at the time of initiation of the procedure. This means that the state of damage must be detected as soon as its sign is detected. Also, in order to avoid pitfall 2 described earlier, the procedure must directly act on the component of concern as Cheung's mobile pumps dealt with reactor cooling component directly (Cheung 1991). This probability of success for the mitigation procedure must be aimed at unity because, for each mitigation scenario, only the successful implementation of such procedure proves that the last line of defence was held against the fatal core melt. A critically significant advantage of the use of this probability aimed at unity for confirmation of the reliability of the process lies in the fact that this probability can be estimated by means of experiment using actual physical and operational systems involved and checked by Monte Carlo simulation based on analytical models of these systems. This approach is the same as that successfully implemented in the aerospace and other high risk industries. In contrast, the approach used in the conventional event tree analysis as depicted in Figure 1 attempts to secure the reliability by aiming at zero or extremely small probability for the core melt event. This, however, cannot be done in statistically acceptable fashion.

The experiments and the analytical simulations described above will be a good subject for future research and development effort.

4. CONCLUDING REMARKS

This paper ventured to recommend some fundamental changes in looking at probabilistic interpretation of low probability but high risk disaster or catastrophe events using Fukushima Daiichi Nuclear Power Plant catastrophe as test- bed. In doing so, for simplicity, an event of uncontrolled reactor core melt is considered as the major cause of catastrophe. Even then, the issue of safety of high risk systems under uncertain hazardous events such as earthquake and accompanying tsunami is significantly complex and defies elaborations on the detailed analysis. Hopefully, however, this paper provides a refreshed probabilistic interpretation of these disasters and catastrophes which are inescapably controlled by probabilistic uncertainty. In this respect, the following issues are worth noting here.

1. The augmented event tree to ensure all the end events perform "core cooled" task with the aid of added events still can be interfered by the type of unthinkable events suggested by Perrow (Perrow 1999) and Beyea (Beyea 1983). How to deal with this issue certainly remains to be the subject of future study. However, in this paper, the augmentation is provided, as an example, by a portable emergency cold reactor core shutdown device that is capable of working directly on the reactor core. This effort directly and actively deals with the reactor core to rapidly terminate the core melt process. Thus, it serves as another, but not incremental, layer of strategic defence against the core melt driven catastrophe notwithstanding the difficulty to bring the device to the core.

2. It is not clear if there is or there will be a technology to cold shut down the reactor core in the process of melting at any stage. If no prospect is in sight for this technology, many suggestions made

in this paper are moot. However, at the same time then, the nuclear power technology will be deemed immature to be utilized. To this disappointment, add the difficulty to get around the unthinkable events, and the controversy over the nuclear waste storage. Then, the proponents of nuclear power generation do not have an easy task to prevail. On the other hand, it appears fair to say that it is premature to abandon the nuclear power technology at this time for complex socio-economic reasons. In addition, it is clearly premature to abandon the research and development for safer nuclear power technology for both existing and new generation plants throughout the world. Knowing the potential catastrophe could impact also throughout the world, importance of the research and development is not a concern of one nation.

ACKNOWLEDGEMENT

The author acknowledges valuable data and encouragement by Professors H. Kameda, N. Meshkati, Y. Kawata, and K.P. Cheung.

Many thanks to my research staff and graduate students at UCI for the details.

REFERENCES

Beyea, J., 1983, Second Thoughts, Nuclear Power: Both Sides, Kaku, M. and Trainer, J., Norton paperback

Cheung, K.P., 1991, A Proposed Backup for Emergency Heat Removal System for Nuclear Power Plants Using Mobile Pumps and Liquid Chilling Units, ASHRAE Transactions, vol.97, Pt. 1, New York

Cheung, K.P., 2012, Innovative Cooling Technology for Combating Extra-large Heat Generation Situations in Nuclear Power Plant Accidents/Incidents, http://icee.hku.hk/index/index.html

Kawata, Y., 2012, The Great East Japan Earthquake as A Catastrophic Compound Disaster, Verification of The Great East Japan Earthquake, Faculty of Safety Science, Kansai University(eds.), Minerva shobo, pp.1-31 (in Japanese)

NISA and JNES, 2011, The 2011 off the Pacific coast of Tohoku Pacific Earthquake and the seismic damage to the NPPs

Perrow, C., 1999, Normal Accident, Princeton University Press