Transactions, SMiRT-24
BEXCO, Busan, Korea - August 20-25, 2017
Division IX (include assigned division number from I to X)

DEVELOPMENT OF SEISMIC COUNTERMEASURES AGAINST CLIFF EDGES FOR ENHANCEMENT OF COMPREHENSIVE SAFETY OF NPPS - PART 1: CONCEPTUAL STUDY ON IDENTIFICATION AND AVOIDANCE OF CLIFF EDGES OF NPPS AGAINST EARTHQUAKES

Tsuyoshi Takada[1], Tatsuya Itoi[2], Takenori Hida[3], Ken Muramatsu[4], Hitoshi Muta[5], Osamu Furuya[6], Keisuke Minagawa[7], Hidemasa Yamano[8], and Akemi Nishida[9]

1 Professor, Department of Architecture, The University of Tokyo, Japan
2 Assoc. Professor, Department of Nuclear Engineering, The University of Tokyo, Japan
3 Assist. Professor, Department of Architecture, The University of Tokyo, Japan
4 Professor, Department of Nuclear Engineering, Tokyo City University, Japan
5 Professor, Department of Nuclear Engineering, Tokyo City University, Japan
6 Professor, Department of Mechanical Engineering, Tokyo Denki University, Japan
7 Assoc. Professor, Department of Mechanical Engineering, Saitama Institute of Technology, Japan
8 Senior research engineer, Japan Atomic Energy Agency, Japan
9 Senior researcher, Japan Atomic Energy Agency, Japan

ABSTRACT

The Fukushima accident in 2011 indicates that any possible events beyond design basis should have been explored deeper and been taken into consideration toward safety improvement of existing nuclear power plants (NPPs) against external hazards. This directly leads that the seismic safety of NPPs should be treated as whole systems with great consideration of interrelations among all constituent elements since the plants are very complex systems consisting of building structures, equipment, off-site surroundings and humans operating and managing all sub-systems (SSCH: Structures, Systems, Components and Humans). In this 3-year project, the nuclear power plant system is analyzed in a cross-cutting approach, and the required performance of both the whole system and the constituent elements during earthquakes are clarified and finally integrated in a systematic manner, then the cliff edges relevant to each performance are identified and be quantitatively assessed. Various possible countermeasures for avoiding and mitigating the cliff edge effects are intensively developed. The paper, first of all, defines cliff edges either in a physical context or in a knowledge-related context, where the latter may be directly related to limitations of currently available knowledge, limitations of used theories and analyses for complex phenomena. Then, the paper demonstrates how to treat these cliff edges in conjunction with the required performance in a plant level during earthquakes. Finally, these cliff edges are integrated into the total plant safety and compared each other to secure the total safety of NPP against earthquakes.

1. INTRODUCTION

The Fukushima Daiichi NPP accident has brought up many important lessons for future safety enhancement of NPPs, as can be seen in current post-Fukushima activities being conducted in many countries. Key issues are implementation of risk-informed approaches, performance-based consideration of a total system as well as sub-systems, explicit inclusions of various underlying uncertainties associated with external natural hazards, behavior of huge and complex NPP systems including human actions. In order to capture the behavior of the total NPP systems subjected to earthquakes, multi-disciplinary approach from soil, structural, mechanical and system engineerings and human engineering, all of which are closely related each other for reducing the risk of NPPs. The Fukushima accident in 2011 indicates that any possible events beyond design basis should have been explored deeper and been taken into consideration toward safety improvement of existing nuclear power plants against external hazards. This directly leads that the seismic safety of NPPs should be treated as whole systems with great consideration of interrelations among all constituent elements since the plants are very complex systems consisting of building structures, equipment, off-site surroundings and humans managing all sub-systems (SSCH: Structures, Systems, Components and Humans).

The behaviour of the NPP system can be characterized in terms of the prominent cliff edges (CEs) in many aspects. Risk management is indeed a number of effective processes of avoiding and controlling potential CEs that the system possesses. Some of CEs can be easily identified and could be controlled directly, but some can neither be even recognized nor be treated in an appropriate manner. Since external events like earthquakes have large uncertainty in nature to the safety of NPP, optimum combinations of countermeasures associated with each CE have to be sought. These are implemented at least three ranges of domains, design, accident management and disaster prevention domains.

In this 3-year project, the nuclear power plant system is analyzed in a cross-cutting approach, and the required performance of both the whole system and the constituent elements during earthquakes are clarified and finally integrated in a systematic manner, then the cliff edges relevant to each performance are identified and be quantitatively assessed. Various possible countermeasures for avoiding and mitigating the cliff edge effects are intensively developed. The paper, first of all, defines cliff edges either in a physical context or in a knowledge-related context, where the latter may be directly related to limitations of currently available knowledge, limitations of used theories and analyses for complex phenomena. Then, the paper demonstrates how to treat these cliff edges in conjunction with the required performance in a plant level during earthquakes. Finally, these cliff edges are integrated into the total plant safety and compared each other to secure the total safety of NPP against earthquakes.

2. PROJECT OVERVIEW

This 3-year project, treating an NPP as a total system to assure safety of the NPP, based on the risk concept and defense-in-depth (DiD) concept, identifies various types of CEs and explores countermeasures by employing hard and/or soft technology to the CEs.

Due to the 2011 Tohoku earthquake and tsunami, the Fukushima Daiichi NPP leaded to the serious accident consequence with loss of entire power supply because of the strong ground motion and high tsunami waves simultaneously. This accident resulted in the serious large accident since the total plant system fell into the state of CE, due to combined causes of failures of SSCs and operators, such as failure of equipment, i.e., loss of emergency diesel generators, organizations not requiring training against SBO (Station blackout), and error associated with the original plant design.

NPPs are very huge, complex systems consisting structures, equipment, various systems, and operators. Therefore, in order to prevent accidents due to earthquakes, the plants themselves should be evaluated as total integrated systems. It is strongly emphasized in this project that the total plant systems are now composed with SSCHs, i.e., structures (S), systems (S), components (C) and human (H). Considering possible release of radioactive materials from the site to the surrounding area in case of severe accident like core damage, disaster prevention planning for the wider region would be needed. To do so, various CEs associated with SSCHs should be identified and possible measures to avoid them should be explored.

According to the above, it is considered essential in the project to identify and develop countermeasures against the potential CEs. The project plan now focuses on the following tasks.

1) Comprehensive categorization and systematization of required performance of the plant

2) Identification of and development of countermeasures against CEs of plant under earthquake condition
3) Development of implementation strategy for safety enhancement of NPP

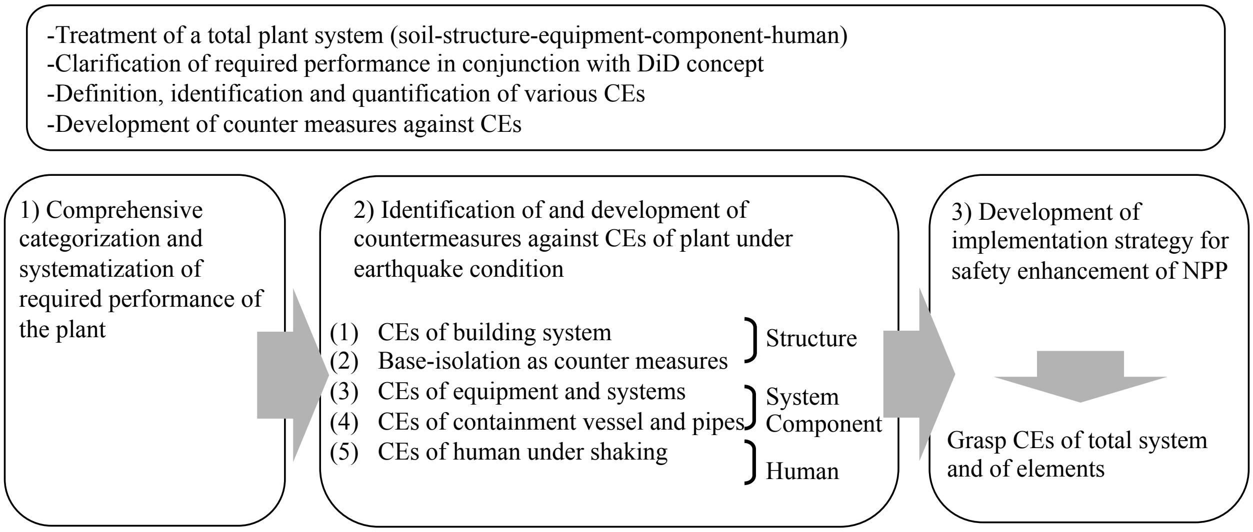

Figure 1 Project Plan

3. DEFINITION OF CLIFF EDGES

In the project, two kinds of CEs are first proposed and clearly defined as in the followings; physical CEs and knowledge-oriented CEs. The former CEs are the ones that have often been meant so far, while the latter are newly defined CEs that have been proposed first in this project. The Fukushima Daiichi accident could be understood as phenomenon un-experienced before, which stemmed from the limit of our imagination. When studying the safety of NPPs, these two kinds of CEs can be properly taken into consideration for almost all treatment of phenomena, modelling and data interpretation and so on.

It is somewhat vague how the physical CEs are defined. According to the definition of the literature (NEI, 2013), the CEs represent the phenomenon that there occurs the significant increase of consequence due to a small amount of decrease of the occurrence frequency of the external event. In the seismic situation, the significant sudden change of the physical state of a system when the ground motion becomes a little larger. This definition of CEs can be understood as depicted in the risk curve, i.e., a relationship between an occurrence probability and its consequence, as in the Fig. 2. The examples of the physical CEs are, occurrence of core damage due to a common cause failure brought by large earthquakes, the impact of base-isolated structure on the outer wall, etc.

On the other hand, the other CEs are associated with the knowledge limit within which we can deduce and make reliable decisions on the basis of our certain amount of knowledge and available information of an objective of interest. It relates the limit of our knowledge domain, the limit of our theory relied on, as expressed in Fig. 3. These CEs imply the deviation from the known domain to the unknown domain or phenomena unexpected.

The theoretical model representing physical states can be understood as an ideal logical system depending on knowledge, idealization and many theoretical assumptions. The model in nature does not work well in the domain that our knowledge cannot cover, the idealization and the assumptions cannot directly be applied to. Once the above condition cannot be satisfied, we encounter a kind of CE associated with our knowledge and modelling, and we may have significant consequence epistemologically as well as physically. Therefore, we cannot guarantee our confidence for elaborately built theoretical domain if the CEs are encountered. These CEs are related to the epistemic uncertainty in the current PRA procedure, which represents uncertainty due to the lack of information and insufficient knowledge, etc. In other words, emergence of the knowledge-oriented CEs result in the unexpected increase of uncertainty, which may invalidate basic assumptions and violate the theoretical basis.

These CEs include nonlinear behaviour or complex behaviour of a system, which cannot be expressed appropriately with a simple linear model. A one-dimensional simplification assumption cannot justify three-dimensional behaviour of a system. Events and phenomenon beyond our imagined pre-specified basis can impair our basic assumptions, idealization and confidence in our analyses.

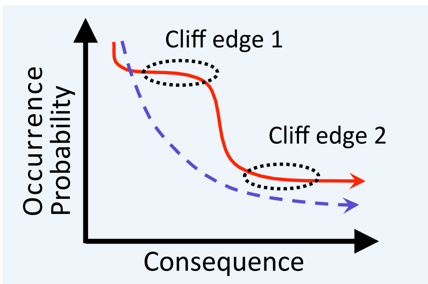

Figure 2 Physical cliff edges

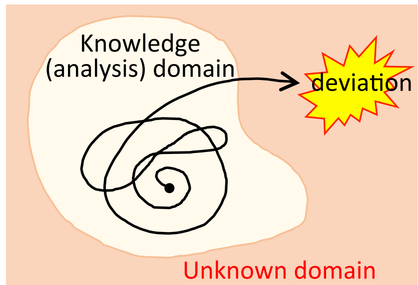

Figure 3 Knowledge-oriented cliff edges

4. CLIFF EDGES OF FUKUSHIMA ACCIDENT

The gigantic 2011 Great East Japan Earthquake occurred with an earthquake magnitude 9.0, which is the super mega earthquake in the Japanese earthquake observation history. A nuclear accident has occurred at the Fukushima Daiichi NPP as the result of the giant earthquake and tsunami of the Great East Japan Earthquake. It was a typical multiple hazard disaster to the plant, where there were large ground shaking due to the main shock and the following tsunami wave, both of which heavily damaged the plant as in the following. While the details of the accident still remain to be fully investigated, the accident is outlined below from the viewpoint of the three fundamental rules for ensuring safety of nuclear power plants during nuclear plant emergencies, i.e. “Stop”, “Cool down”, and ”Confine” (Takada, 2011).

As the result of the ground shaking during the earthquake, control rods were firmly inserted into the cores of reactors, Nos. 1, 2, and 3 of the Fukushima Daiichi NPP, all of which were operating at the time of the earthquake, as a part of the automatic shutdown procedure, and thus the first rule of "Stop the reactor" was accomplished as originally designed. However, as the result of the earthquake, an accident developed as shown in Fig. 3, where the roman numerals in bracket indicate the order of accident sequence. (i) Off-site electric power was rendered impossible, and thus the plant's emergency diesel generators were activated and the emergency core cooling systems began operating. Approximately one hour later after the earthquake, a giant tsunami of about 14 meters in height hit the plant, (ii) incapacitating diesel generators and seawater pumps, (iii) making it impossible to remove the decay heat of the core fuel to cool it down. Then, (iv) the plant lost the on-site power, and then despite water injection into the reactors, fuel failure occurred. Some damage to the pressure vessels and containment vessels is deemed to have occurred, and (v) hydrogen explosions occurred due possibly to the accumulation of hydrogen within the reactor buildings. As a result, radioactive material had been released from the reactor buildings and reached areas outside the plant's premises. In other words, cooling and containment of the nuclear reactors were not achieved, and as a result, radioactive material from the plant has been released to areas outside the plant site and contaminated the surrounding areas.

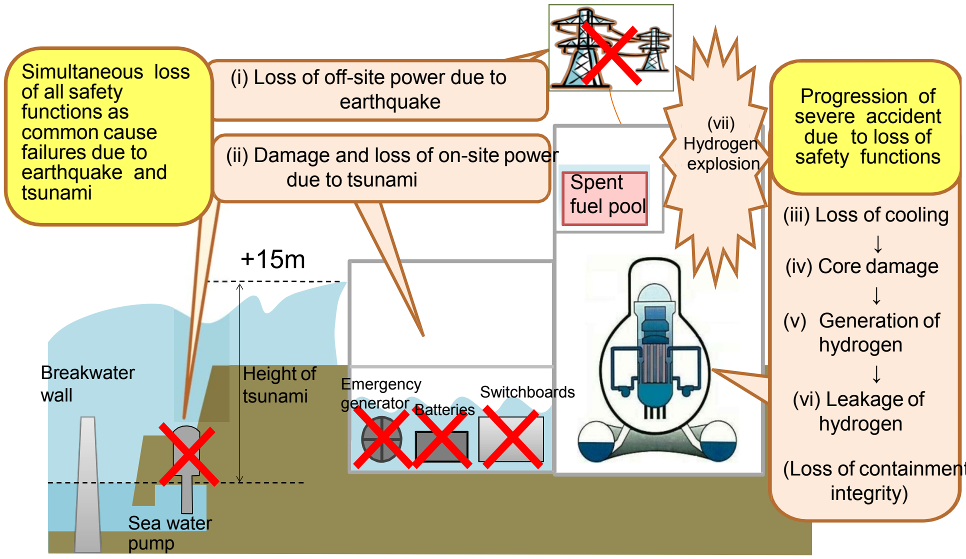

Figure 4 Accident Progression (NRA, 2012)

According to the above accident progression, there were several CEs that can be observed. Some can be categorized into physical CEs, some are into the knowledge-oriented CEs. In the following, these CEs are discussed along with the concept of Defense-in-Depth (DiD) concept that is expected as the basis of effective counter measures to the CEs.

5. DEFENSE-IN-DEPTH CONCEPT

An aim of ensuring safety of NPPs is not to become apparent the influence of the radioactivity (radioactive materials). Almost all radioactivity of the NPP are enclosed in the fuel in the nuclear reactor. Keeping this radioactivity enclosed during normal operation and not affecting significant influence by the radioactivity to the vicinity in the postulated accident are the aims of the nuclear safety. This concept can be applied to ensuring safety of NPP when being hit by natural disasters such as an earthquake and or the tsunami.

There is concept of “Defense in Depth” as a basic strategy for ensuring safety in the nuclear energy systems. This is applicable not only for the nuclear systems, but can be applied generally as concept of ensuring safety of safety critical facilities. In addition, the DiD is fundamental concept defining the measures which should be taken to achieve the nuclear mission of ensuring safety to protect people and the environment. There are several different protection levels in the DiD, and even if one protection level was damaged, the overall safety must not be threatened by that.

According to IAEA (1996), the following description on the DiD is now referred to as below and five levels of DiD have been proposed as defined in Table 1.

> *“… all safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. DiD consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for*

some barriers, in accidents at the plant. DiD is implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant."

Table 1: Levels of Defense in Depth (IAEA, 1996)

Level of DID	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident management
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequence of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

The levels of DiD can be specified in terms of sudden change of system states, which may be called "cliff edge effects". Figure 2 illustrates some cliff edges that indicate critical states as a sudden increase of the NPP consequence. These CEs corresponding to the plant critical states can be treated as physical CEs. To diminish the adverse physical states of the plant, and those of SSCHs, effective countermeasure for each element based on the CEs should be sought. The DiD concept is expected to work well to diminish these physical CEs against external disturbance.

On the other hands, it is problematic to reduce and avoid the knowledge-oriented CEs. What could be the DiD concept to treat these CEs like? The DiD concept for them should also be sought in this project.

6. IDENTIFICATION AND AVOIDANCE OF CLIFF EDGES

It is possible to capture realistic seismic behaviour of NPP buildings, equipment, systems and operators, and clarify the relationship among CEs of individual elements as well as the plant system. The CEs of the whole plant could be identified by applying a procedure similar to the stress test conducted after the Fukushima accident in Japan. Namely, by increasing seismic input to the plant, a conditional probability of performance failure, i.e., a seismic fragility curve of each element as well as a seismic fragility curve of the whole plant system with paying great attention to interdependency of those of other elements, the critical CEs among many CEs of the plant system could be identified. Use of expression of the fragility curves can drastically enable us to take account of various possible combinations of the states of individual elements, so called "accident sequences", and their occurrence frequencies. CEs associated with individual elements such as SSCHs will be studied, and then CEs of the total plant system based on the categorized required performance will also be identified and quantified in the other papers.

Effectiveness of application of base-isolation devices to safety critical buildings will be studied from the viewpoint of avoidance of the relevant CEs. It is expected that the application of the base-isolation technology can mitigate CEs not only of SSCs but also of human. Physical as well as knowledge-oriented CEs will be able to be avoided by using the base-isolation technology. Figure 5 illustrates that fragility curves associated with potential CEs selected in different constituent elements for the presumed plant performances are drawn. It is demonstrated in the figure that to accomplish the required performance of the plant during earthquakes, many elements cooperate with each other to moderate more significant CEs in the plant level. From the comparison of relevant CEs of a non-base-isolated plant and those of a base-isolated plant, application of the base-isolation technology drastically avoid the potential CEs and largely increase seismic safety in a physical sense, and moreover can put the isolated buildings, pipes and equipment installed in the buildings, and even operators in the main control room into a small range of dynamic responses where the response can stay in an elastic region. This is indeed not only the avoidance of physical CEs, but also the avoidance of knowledge-oriented CEs since we do not have to take account of additional uncertainty related to nonlinear response of equipment.

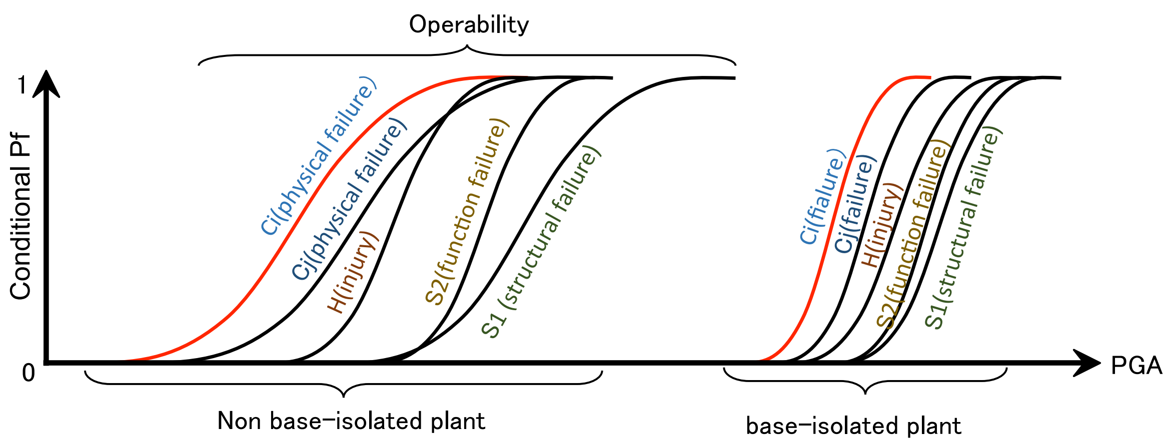

Figure 5 Fragility expression of base-isolated plant

7. CLIFF EDGES BASED ON DEFENSE-IN-DEPTH CONCEPT

Control of the CEs is the process of selection and implementation of an optimal alternative among various risk reduction measures, and the results should be reflected to design and be utilized to multiplication and diversification of safety systems towards enhancement of the total system in case of accidents. Risk concept is effective concept to capable of explicitly treating various uncertainties and of consistently dealing with multi-disciplinary technical fields related to NPP safety. Here, taking earthquake and tsunami case as external hazards, risk-informed earthquake and tsunami protection scheme is developed together with the concept of IAEA-proposed DiD.

As a proposed framework for securing NPP safety against earthquakes and tsunamis, risk concept and DiD concept are now integrated into an risk management framework of NPP, as given in Fig. 6 (JAEE, 2015), which are partially refereed to from the literature (USNRC, 2013). It can be observed from the figure that the three domains; design, AM (accident management) and disaster prevention and mitigation, are clearly classified, and that each domain corresponds to the level of DiD as seen in the left vertical bar. In the probability-consequence diagram, the ranges of conventional Probabilistic Risk Assessment (PRA) levels are also overlaid, where the level 1 PRA focuses on the core damage frequency (CDF), the level 2 PRA targets the containment failure frequency (CFF) and the level 3 PRA concerns the large early release frequency (LERF), along with the performance goal and the safety goal, both of which are expressed in terms of the annual frequency in the vertical axis. As discussed earlier, the first three levels of DiD ("stop", "cool" and "confine") have been clearly stated as fundamental safety principles with great confidence before the Fukushima Daiichi Accident. Additional two more levels (levels 4 and 5) in DiD are placed, namely, the appropriate management of accident beyond design basis, and prevention measure and emergency response for safety of the public and environment.

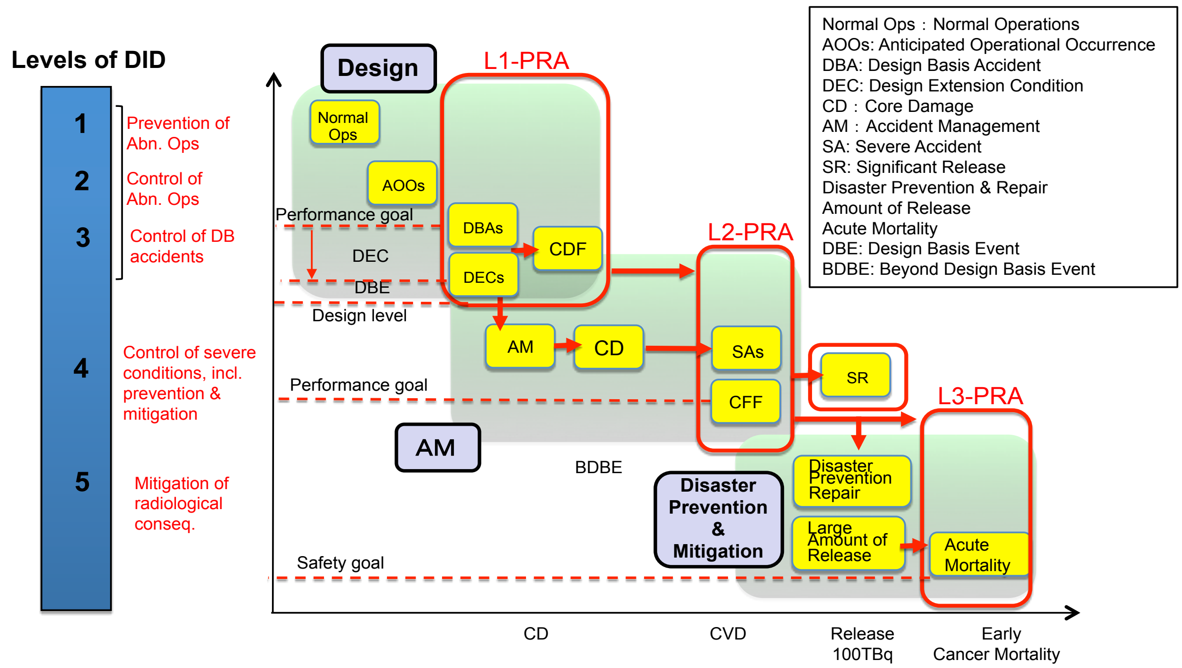

Figure 6 DID and Performance Requirements for NPP (JAEE, 2015)

8. CHALLENGES

Common cause failure (CCF) effect is the biggest issue to keep each level of DiD independent during highly extremely severe conditions. When a main system fails under large shaking condition, its back-up system may also fail. Therefore, the back-up system would be no more effective in this case. It is not easy to keep the levels of DiD independent under large seismic excitation condition. One proposes the three important characters of the levels of DiD; multiplicity, independence and diversity of relevant safety systems. Sill it would be difficult to make the DiD concept fully effective under earthquake conditions, which is addressed as one of future challenges.

After the Fukushima Daiichi accident, tremendous amount of recovery operations made by human beings in and around the site has been employed to stabilize the accident until now. These contributions by the human operations have never been counted in the conventional safety assessment so far. This human commitment should be appropriately taken into consideration in the safety assessment for more realistic assessment.

9. CONCLUSIONS

This paper presents the 3-year project on CEs of NPP systems against earthquakes, where the basis of treatment of the CEs, new definition of CEs, application of DiD concept and etc. are discussed briefly. Main features of the project are multi-disciplinary approach, unique treatment of CEs, performance-based consideration. The other companion papers under the same title will follow for more specific study in SMiRT24 conference.

ACKNOWLEDGEMENTS

This study is the part of the result of "Development of Seismic Countermeasures against Cliff Edges for Enhancement of Comprehensive Safety of NPPs" carried out under the Center of World Intelligence Project for Nuclear S&T and Human Resource Development by the Ministry of Education, Culture, Sports, Science and Technology of Japan.

REFERENCES

Takada, T. (2011), *What engineering should be after the Unprecedented Disaster?* WG for Emergency Engineering Vision, School of Engineering, University of Tokyo

Nuclear Regulatory Agency (2012), https://www.nsr.go.jp/english/index.html

IAEA (International Atomic Energy Agency) (1996), *INSAG-10 - Defence in Depth in Nuclear Engineering*

JAEE (Japan Association of Earthquake Engineering) (2015), *Tsunami Resistant Engineering for Nuclear Safety – Toward an Integrated Framework for Earthquake-Tsunami Protection-*

USNRC (2013) *NUREG-2150: A Proposed Risk Management Regulatory Framework*