E-Journal of Advanced Maintenance Vol.8 No.4 (2017) 57-65
Japan Society of Maintenology

Development of Resilience Evaluation Method for Nuclear Power Plant

(Part 4: Concept of System Safety on Operating Nuclear Power Plant)

Hosei University	Hiroshi, MIYANO	Member
University of Tokyo	Akira, YAMAGUCHI	Non-member
University of Tokyo	Kazuyuki, DEMACHI	Member
Osaka University	Takashi, TAKATA	Non-member
Atomic Energy Society of Japan	Shigeki, ARAI	Non-member
Mitsubishi Research Institute, Inc.	Naoki, SUGIYAMA	Non-member

Abstract

The total system design of a nuclear power plant ensures "Nuclear safety" through making practically achievable efforts to prevent and mitigate nuclear and radiological accidents. The performance based system design with "Defense in Depth (DID)" has been laid out as the key means to "preventing accidents", "controlling escalation to serious consequences", and "mitigating impact to the public". DID is extended to the management of severe accidents, and is an approach intended to provide protection against the development of a wide variety of events by means of redundant, diverse and independent protective barriers.

By combining the concepts and risk assessment discrete "Defense in Depth", it can be expressed as a risk level corresponding to the degree of each layer of the DID. A Situation that exceeds the normal operation becomes an abnormal situation in which more than even the design criteria, various AM measures are taken. The ability of the resilience to recover the function until the required function, and quantified in risk level as a safety corresponding capability of the system, are expressed as a resilience index.

By using the resilience index, safety capability of the plant system can be quantitatively grasped, that whether the safety by the AM measured is how much improvement, what is good to select which means, etc. it can be used for the decision.

Keywords: Resilience Index, Safety Assessment, Severe Accident, Accident Management, and System Safety

1. Introduction

In Japan, there is the threat of a variety of natural disasters. On July 16, 2007, an earthquake occurred in Niigata-ken Chuetsu-oki and the TEPCO Kashiwazaki-Kariwa nuclear power plant was affected. Following the sensational headlines of a nuclear power plant disaster that showed a video of a transformer on fire, a feeling of insecurity among the general public concerning the safety of a nuclear power plant, when faced with an earthquake, has spread. However, a subsequent investigation of the Kashiwazaki-Kariwa nuclear power plant on nuclear safety revealed that all of the units were stopped safely, and that no particular problem arose because of this.

On the other hand, on March 11, 2011, a tsunami, which was generated by an earthquake of magnitude 9 off the Pacific coast, hit nuclear power plants in five locations in the Tohoku region. Reactor No. 1 of the Tokyo Electric Power Company in Fukushima released a large amount of radiation which became an unprecedented major accident.

The Society experienced how the risk of nuclear power can be actualized. It revealed that an earthquake can cause a serious disaster, not only by vibration propagation, but also other phenomena that accompany such an event, for example, tsunamis and landslides. This new experience led us think about our commitment to risk when it comes to natural disasters.

Contact: Hiroshi Miyano, R1309, Hosei University Graduate School of Design Graduate School of Engineering, 72-21 Horikawa-cho, Saiwai-ku, Kawasaki-shi, 212-0013
E-mail: hiroshi, Miyano.77@hosei.ac.jp

The Fukushima Daiichi nuclear power plant accident clearly shows that the use of nuclear energy is accompanied by risk and that the nature of the threat or how to prevent it from developing into a nuclear accident at a power plant is an important issue. Furthermore how to prevent the development of the nuclear accident caused by a variety of natural phenomena, has become an important problem.

Previous designs decide the specifications required for the equipment according to safety design by performing reliably to ensure design criteria where the most important aspect is that the safety of nuclear energy is assured. Such a design has significant limitations.

From now on, the design, normal operation, detection of abnormalities, how to respond to abnormalities, will accord to levels; ranging from the first level of "defense in depth" in response to a situation that exceeds the design criteria along with an emergency response (Disaster Prevention) up to the fifth level, where an equal amount of safety design is required. The design will be obtained with the aim of optimizing the system as a whole where it defines the common evaluation index. This will provide a safer system. In addition to post-accident response and recovery, it is important that those aspects related to safety go on to include reconstruction, also. This recovery, entire reconstruction, and the consideration in advance of including the accident occurrence factors that lead to the accident, form the basic concept of nuclear safety resilience – a new design proposal.

2. System safety concept

The boundary between labor and safety has become ambiguous, and adds to the important task of responding to natural disasters. At nuclear power plants, where safety measures have become more complex, the securing of "nuclear safety" as a system of the entire power plant must be considered. Regarding the systematic checking of safety, see Fig. 1 below for an overview of the structure[1].

Regarding the category of design, there is a mechanism to evaluate whether the safety aspects of a nuclear power plant are being properly maintained or not. In other words, resistance against natural disasters is required, especially in a country such as Japan that experiences earthquakes and tsunamis, volcanic activity - where these hazardous threats may damage a nuclear power plant. When looking at the basic safety functions that nuclear power plants have as a system, together with related functions, the reliability of safety functions maintenance is evaluated. The deterioration of a function, as a system, according to the deterioration and lifespan of materials, is evaluated, and according to this one can then ask as to how much reliability has been reduced. Thus, as a response to when the system is operational, through incorporating elements of conservation, what kind of conservation in reality - replacement of material, inspection and the improvement of the equipment - should be installed in order to prevent the deterioration of function, and as to whether or not it is possible to indicate that reliability is assured.

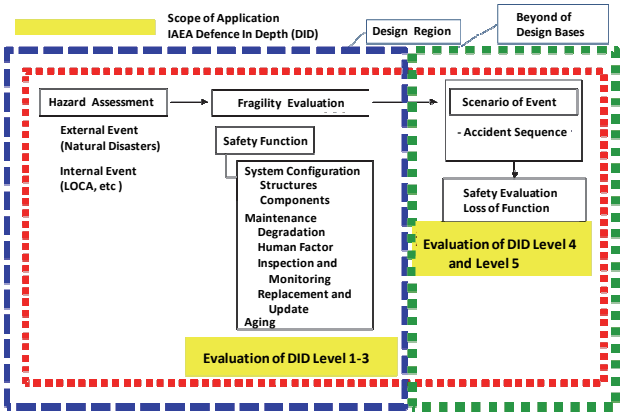


Fig. 1 Concept of Safety Evaluation on Design Phase and Beyond Design Phase

When dealing with an area of response to a situation that exceeds the limit of the design, working on the assumption that natural phenomena are also unpredictable situations, that go beyond previous assumptions, that is, situations that exceed the design condition limits, a response should show that a variety of preventative measures leading up to an accident at a nuclear power plant are being taken. Situations that exceed the design limits are not uniformly specified. Assuming a variety of factors, it is necessary to consider measures for a variety of possible scenarios. When taking measures following such situations, we must ensure safety to obtain sufficient resistance.

3. Safety as a result of "defense in depth"

"Defense in depth" is the most important and basic idea or concept concerning "nuclear safety", and it has been recognized as a common concern throughout the world. The idea is to offer an effective and a variety of realistic strategies, along with their appropriate combinations to ensure safety. Both up until now, and in the future, the significance and role of these strategies will not change. Insight into "defense in depth" and a risk assessment

relating to combined beneficial safety can be obtained. [2]

3.1 Nuclear energy and safety assurance

Basic nuclear power safety, originally, is to effectively minimize the amount of risk that human beings could be exposed to when there is a large amount of inherently dangerous radioactive substance that is released through the environment or comes into direct contact with people.

Many facilities, within the system and their design, prevent the damage or destruction of equipment, of course, and for the people who use them. Sufficient consideration is taken into account so as not to adversely harm those in the vicinity. In many cases, the inclusion of quality management and design according to stringent conditions are implemented to secure "nuclear safety." Design and construction of a nuclear power plant, day-to-day operational management and security have been ensured in the following manner.

3.2 Ensuring safety in a nuclear power plant design

Firstly, from the viewpoint of preventing an abnormal occurrence, sufficient margins and quality assurance and improved inspection tests are included. Secondly, when it comes to full monitoring of abnormal occurrences, furnaces are stopped in the first instance, thereby preventing the spread of an abnormal accident. Thirdly, in the event of a situation that may lead to an accident, in order to reduce the influence of the accident to that of minor, sufficient cooling and the successful confinement of radioactive materials is carried out. As a result, in order to prevent a nuclear accident - following a nuclear accident, radioactive substances are released from the facility to the outside, and this will relate to the affects radioactive materials may have on people - a variety of measures are put in place. In this way, because of "multiple protection", nuclear power is "safe."

Both of these are mechanisms of defense in depth found in the design of a nuclear power plant, and are mechanisms that have been set in place in order to avert an accident within an expected range.

3.3 Countermeasures to a situation which exceeds the design conditions

The essence of defense in depth is to consider the countermeasures in the event that assumptions are exceeded. That countermeasure against the tsunami, which was excessively beyond expectation in the Great East Japan Earthquake, showed us that insufficient strategy towards unexpected situations can cause severe accidents. The defense in depth indicates the most important concept of ensuring that safety from the viewpoint of preventing nuclear accidents and from the objective of safety, which must be observed eventually from the point of view of the countermeasures towards those events, when it was designed, within the ranges of assumed designs and beyond the ranges of the design condition. This idea of ensuring safety is applicable to other situations, and not only nuclear power equipment per se.

This intends to minimize the possibilities that may lead to a nuclear accident, by not only taking previous assumptions which were considered in the design and ensuring definite safety in the designed conditions, but by also, implementing the safety measures in case of a situation that exceeds the design conditions.

In this way, a situation where nuclear facilities are thought to have caused contamination to people or the environment via radiation, it is eliminated by an effective planned response, whereby even if the accident exceeds the limit of the design, it should be possible to reduce the possibility of a nuclear accident occurring using an appropriate response. Furthermore, in the case that a nuclear accident has occurred, people affected in the surrounding areas, in addition to a "disaster prevention" response that can protect people in a number of ways, a safety mechanism that is responsive from a number of viewpoints is known as "defense in depth."

3.4 Ensure its effectiveness

There are some difficulties in the implementation of the protection level setting and safety measures being based on this because of natural phenomena. It is difficult to foresee the countermeasures of an abnormal situation, for example the lead up to an accident which exceeds the design criteria. In other words it is difficult to cover all of the possible scenarios that can occur under accident management (referred to as AM.)

For example, when it comes to flexibility with portable equipment, it is thought that having a flexible response is effective, but on the other hand, in order to proceed with a variety of accident management measures (AM measures), ability and responsibility that is responsive to the organization and the people, appropriate judgment and leadership are what is required.

As for the implementation of AM measures in a state

whereby a severe accident has actually occurred, it is also clear that there are a number of difficulties when it comes to implementation. For instance, there is a limit in time and space to permit a variety work carried out in a high radiation environment, which causes serious constraint for the operators in the control room. Moreover, some scenarios prepared as AM measures cannot always be implemented under certain accident conditions.

In order that "defense in depth" be the principle of nuclear safety, it is necessary to organically combine training and exercises so as to ensure the effectiveness of AM measures and disaster prevention - along with a large number of factors such as constant review of those mentioned above, and additionally, the carrying out of multiple and diversified safety, including both on and off-site.

4."Nuclear safety" in the system design

4.1 Defense in depth in the design

A Nuclear power generation system is designed, built and operated based on the specification request just the same as other general products. Its reliability and safety, is ensured based on the theory, law and regulatory standards. The idea of the foundation is thought to ensure a "nuclear safety" and the ensuring method by "defense in depth". Thus, each organization must play their part in recognizing a mechanism such as this. The design can be defined to apply appropriately with the operations which are assumed at that time, to ensure safety at the nuclear facilities in use and be verified using analytical evaluation in order to confirm the soundness of the equipment to satisfy the required performance based on the specification request and to ensure “nuclear safety.” Thereby manufacturing equipment and construction, also planning in order to operate and maintain, and modifying the whole, design books should be compiled as drawings and instructions.

4.2 The basic approach to design criteria and design

In nuclear power plant equipment design, the safety design is processed in conjunction with the core design as part of the system design. “Safety design” can be defined through the modification of the overall achievement to ensure nuclear safety through the total levels of protection, by applying the concept of “defense in depth." Also, facilities design can be defined to construct the plant facilities logically with feedback from them. Up until now, the design, the safety design, was primarily considered, up to the third layer of the "defense in depth" safety mechanism, to be important, and the basis of the design for determining the "design basis" has had an important position. Equipment design utilizes layers one through three of defense in depth, and in these, through the provision of equipment of appropriate specification, a plant system that meets the requirements of safety, is built, thus making up the structure. With this, the aim has been to reliably maintain nuclear safety.

In Table 1, an important feature to ensure nuclear safety, namely, front system function, boundary function (to confine), cooling function (to cool), the control function (to stop), other support systems and examples of apparatus and systems to consist it is shown with the classification of safety function of Prevention System (PS) and Mitigation System (MS).

Table 1 Basic Safety Function and System applied to DID

Defense-in-depth level	Boundary	Cooling	Control	Common
Level 1 Normal conditions	Preventing proliferation of fission products in the coolant (PS) Radioactive materials storage (PS) Coolant pressure boundary (PS- Containment of reactor coolant (PS) Maintenance of reactor coolant (PS) Radioactive materials storage (PS) Closure of safety relief valve (PS)	Maintain core geometry (PS) Reactor core cooling under normal conditions (PS)	Prevention of excess reactivity (PS) Circulation of reactor coolant (PS)	**Common factors for Level 2 & 3** • **Issuance of signals to activate engineered safety facilities/ components & reactor shutdown systems (MS)** • **Safety significant items (1) (Emergency onsite power systems) (MS)** • **Safety significant items (2) (Control room) (MS)** • **Safety significant items (3) (reactor auxiliary coolant systems) (MS)** • **Safety significant items (4) DC power systems (MS)**
Level 2 Prevention	Over pressure protection of coolant pressure boundary (MS)	Heat removal after reactor shutdown (MS) Safety shutdown functions outside control room (MS)	Emergency reactor shutdown (MS) Maintain sub-criticality (MS)	
Level 3 Mitigation	Containment of radioactive release [PCV] (MS)	Core cooling (MS) Mitigation of reactor pressure increase (MS)	Maintain sub-criticality (MS) Controlling power output increase (MS)	
Level 4 Accident Management	Radioactive release containment [reactor building, gas treatment] (MS) Severe accident management [PCV event] (MS)	Severe accident management [Make Up Water System, FP systems] (PS)	Severe accident Management (MS)	
Level 5 Accident Management				

There has been no definite concept in general, so far, that copes with a variety of events, especially for external naturally occurring phenomena. If you look at the equipment design on ground motion, based on the various ideas in academia, as a comprehensive response, it defines a method for evaluating the soundness of the equipment which can determine the size of ground motion. The criteria used in the design has been considered as follows. Considering conservatively the threat of natural phenomena to the extent that it is scientifically anticipated, based on past data, the design criteria has been determined quantitatively in order to ensure the structural soundness, even in case of a situation that is beyond the criteria, from the viewpoint of uncertainty. Based on this criterion, the design was processed with ample margin. And, manufacturing and construction were performed based on this design. Similarly,

- design based on data evaluation of other natural phenomena,

such as; tornadoes, volcanic explosions, also threats such as falling meteorites; and physical theory, must be performed.

4.3 The role of the safety design

In a conventional nuclear power plant design, up until the third layer of "defense in depth," firstly the "stopping", "cooling, and the assurance of front system "confinement" was the main idea. However, regarding another important aspect, in response to a situation involving loss of power, functions that govern such a situation and the support system function, it is important to adequately respond to the front system.

Regarding the safety design of nuclear power plants, harnessed system design and a design that satisfies system function, required in the safety design, must be carried out.

In the system design, equipment and piping design, instrumentation and control and electrical design included, all of the equipment is vital. In the system design, abnormal time, to ensure safety at the time of the accident including the power supply and the electrical system, further, it is important to work on a comprehensive evaluation.

This kind of commitment to safety must always allow for review and be robustly responsive.

For safety design, facility design from the first layer of the "defense in depth" to the third layer, and, of course, the fourth and fifth layers should be included. On top of that, the evaluation of required functions must be addressed also in order to introduce the idea of "system safety" in the safety assessment. "In order to ensure the concept of "defense in depth," the safety plan conforms to the whole of "defense in depth," and as proposed in this series' paper, a mechanism built to enable this and for it to be carried out reliably is what is desired.

4.4 The role of AM measures

As a plan basis, with a focus on the internal workings of LOCA, a plan that aims to ensure safety through the bolstering of facilities has been carried out.

Natural phenomena are always accompanied by risk, and while it is difficult to make an accurate assessment, we must fully understand natural phenomena in order to be able to properly evaluate the risk of a nuclear disaster. As for seismic vibration, we started working on evaluating the risk of its after effects, but just as with other events, a risk assessment must be carried out.

In order to reliably ensure safety, we must address anything that is likely to occur that has not been accounted for in the plan.

In other words, as a response to a scenario that has exceeded the criteria, the concept of "defense in depth" will be applied. This measure is known as "accident management" (AM).Within the realm of AM, we allow for scenarios that exceed it, by providing equipment following a plan that considers the diverseness and uniqueness of a scenario. Then equipment that effectively uses AM measures is prepared. In particular, when managing an accident, at an abnormal time when a number of facilities are not used on a daily basis, a variety of scenarios are considered and exercises and training must be reinforced.

5. System safety

5.1 Structure and functions necessary for "nuclear safety"

Table 1 shows the constructs that constitute necessary features of a nuclear power plant, its system and its instruments.

The basic elements required for design consist of: a boundary function, a cooling function and a control function in conjunction with a power supply function (mentioned earlier). These are the important components necessarily underlying a nuclear power plant. A nuclear power plant's design is made up of the maintenance of the appropriate inter-relationship of these functions. It is a system design. Thus for any given event within the design criteria, the soundness of facilities and safety is ensured to be secured. This is the basic concept of system safety.

On the other hand, in the event of a scenario that exceeds the design limit, because the response will differ depending on event and circumstances, all kinds of scenarios are important at this level. In response to the unexpected, effective envisioning of possible scenarios and the preparation of a responsive coping strategy will be necessary. Furthermore, by normalizing and standardizing the equipment and procedures, a mechanism that is systematically responsive is constructed.

5.2 Issues when preparing for an accident

1) Decisions "beyond the design basis"

Structural integrity following seismic vibrations has become an issue. In other words, it means that seismic vibration intensity has slightly exceeded the reference value. For example, when a seismic vibration exceeds the level set by the part of a frequency band, or when the oscillatory waveform exceeds it momentarily, these are recognized as being threats to plant safety and structural soundness. Although seismic vibration at the Kashiwazaki-Kariwa nuclear power plant, following the Chuetsu-oki earthquake, was more than three times the set level, it was confirmed that the soundness of the equipment was fully

intact. It was confirmed that the structural design for seismic vibration had a more than adequately large margin. After that, in nuclear power plants across the country, seismic vibration levels we revised and set to a strict level, thus it can be confirmed that there is still a large margin. Simply put, while the margin for structural soundness has been well received, the margin for functionality is estimated to be even greater.

We must rethink the meaning of "beyond the design. "In other words, even during the Tohoku-Pacific Ocean earthquake, seismic vibration acceleration that just exceeded the set level at a number of nuclear power plants around the East Pacific Ocean Coast was observed. No effects presented themselves in the observed data of a power plant, and the time of earthquake soundness of analytical estimations and from the history of other power plants, was also apparent in a report that was made by the Nuclear Regulatory Commission. Therefore, regarding a scenario that exceeds the level of seismic vibration, it will not simply be a case of revising the, up till now, reference valuation acceleration response, but we should discuss how the vibration response effects the structural integrity and consider an appropriate method of evaluation.

In addition, when setting a limit for tsunamis, from the measured height of the tsunami up to the point where it reaches the power plant, from the least amount of time that it takes, when it is a tsunami that exceeds a set height, we can prepare a response measure and change when to initiate it.

Therefore, we must set a limit which grasps and appropriately judges as to "when it has exceeded the limit" and "to what extent it has exceeded the limit." Having carried out accident management (AM), this is an import decision to make.

2) In response to a scenario that "exceeds prediction"

It is said that the large tsunami that attacked our shores was "unexpected." On the other hand, it is said that the "unexpected," when it comes to nuclear safety, is impermissible. It is not easy to predict a large tsunami that occurs perhaps once in a thousand years. There is the complexity of wave design, from the movement of the earth's crust as well as seismic design, wave generation, propagation, run-up, post evaluation of floods and other phenomena, buildings, and then there is the complexity of equipment structural and electronic instrument design. A variety simulations and estimates are carried out for a variety of tsunami sizes. Even if the size is set, a tsunami that exceeds this may not come, but the guarantee of it not coming cannot be assured. Degrees will vary, similar to those of ground motion, thus a response that assumes it will exceed these sizes is required. For a variety of natural disasters, a creative approach is required.

However, in response to the unexpected, when it comes to "defense in depth," a response that exceeds the design criteria can be carried out, for example, with respect to uncertain, new and big natural disaster threats, however, whether it can be said that measures can be taken, or that they are acceptable is a difficult challenge. Whether or not there is a new hazard, or whether the response measures are appropriate, it is always important to question and to continue making revisions.

6. Initiatives for a new system safety design

Facility design is sought having been approved by management, whereby management investigate equipment design and disasters. But plant safety cannot fully address facility design alone. The design, with AM measures, across different disaster prevention measures, it is important to construct a concept of a new kind of nuclear safety with functionality at its core.

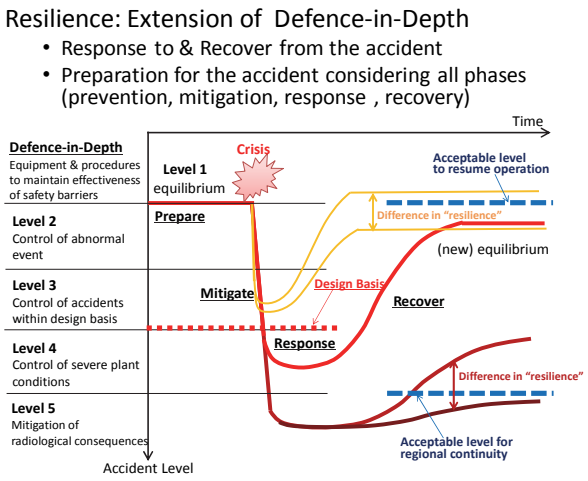


Fig.2 Concept of Resilience and D-I-D

Design plays an important role. In order to properly maintain "nuclear safety."

In order to properly maintain "nuclear safety," it basically must be based on the safety design in accordance with the concept of "defense in depth." The design, the response to the different dimensions of level 1 - 5 of the IAEA's "defense in depth" have been aligned and optimized and the mutual cooperation of equipment design principles of level 1 - 3 and level 4 and the management principles of level 5 is important. There must be a

safety mechanism that, as a system, combines functions required by the plant.

In the design of a nuclear power generation system, it is a total system that takes into consideration a combination of the entire system, such as the ground, buildings, equipment, piping, electrical apparatus and instruments. From a total process perspective serving as a mechanism that takes into account normal day-to-day running of the plant to a state of emergency, management consisting of all areas of "defense in depth," it is a total management design that optimizes both software and hardware. Integrating all of these comprehensively, it needs to be a total design that has a holistic approach.

Measures that take into account a number of scenarios, function recovery measures should be prepared for in advance. In fact, the size of the impact is expressed by the level of safety function, but corresponds to the reliability as a concept, which is the opposite of risk value. It is the level of risk.

The basic concept of resilience [3] from these normal "provisions" to "preventative measures," "grasping of the conditions," "AM and recovery" and the "maintenance of a new equilibrium state," point to a wide response. And this resilience index, while considering these circumstances, shows to what extent each response measure's capability is. Starting with the evaluation of an abnormal occurrence, whether or not it leads to the occurrence of an accident, and the response that is taken when an accident occurs, as a result, to what level is recovery achievable. Then the efficacy of the processes which respond to a number of accidents are combined and an attempt is made to show, as an index, to what extent a plant may be resilient.

7. Conclusion

By combining the concept and the risk assessment of discrete "defense in depth", the occurrence of a situation that exceeds the normal operation, becomes an abnormal situation which exceeds even the design criteria. A variety of AM measures are taken and the amount of recovery resilience for necessary functions, where the level of risk that corresponds to that degree can be expressed. In this way the system's safety response capability is quantified as a risk level, and an evaluation method of necessary capacity for safety which appears as a resilience index was proposed.

By using the index of such resilience, safety capability of the plant's system can be quantitatively grasped, and it is possible to see as to what extent safety, according to the AM measure, is achieved. Then, the best method can be chosen, which can then be used to inform a decision.

Acknowledgments

This study is a part of the result of "Study of the comprehensive safety evaluation method of the aging plant," (Mitsubishi Research Institute was commissioned by the Nuclear Regulatory Agency as aging technical evaluation business for innovation). Herewith, we would like to show our gratitude.

Citations

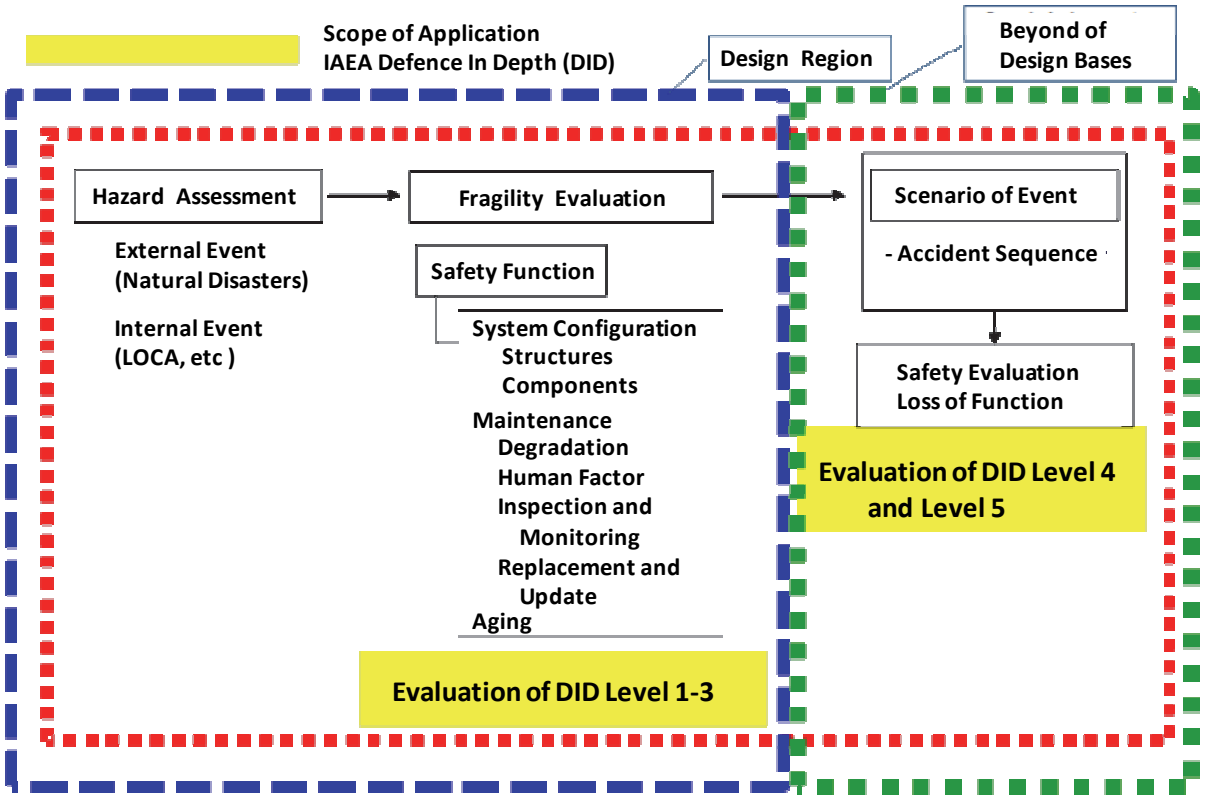
[1] Investigation Committee on the systematization of wave engineering for Nuclear Safety: "Nuclear wave engineering for safety - a comprehensive technology system of the earthquake and tsunami defense" Japan Association for Earthquake Engineering, Nuclear Society (2015).

[2] The Atomic Energy Society of Japan (2014): recommendations for tomorrow and the first nuclear power plant accident - the whole picture of Fukushima, Society Gikocho report, Maruzen Publishing (2014).

[3] N. Sekimura, H Miyano, T Itoi,. "Resilience: Engineering: New Discipline for Enhancement of Nuclear Safety", Short Paper of ICMST-Kobe **2014,** pp.85-90, (2014)

(27,7, 2016)

8



Defense-in-depth level	Boundary	Cooling	Control	Common
Level 1 Normal conditions	Preventing proliferation of fission products in the coolant (PS) Radioactive materials storage (PS) Coolant pressure boundary (PS- Containment of reactor coolant (PS) Maintenance of reactor coolant (PS) Radioactive materials storage (PS) Closure of safety relief valve (PS)	Maintain core geometry (PS) Reactor core cooling under normal conditions (PS)	Prevention of excess reactivity (PS) Circulation of reactor coolant (PS)	**Common factors for Level 2 & 3** • **Issuance of signals to activate engineered safety facilities/ components & reactor shutdown systems (MS)** • **Safety significant items (1) (Emergency onsite power systems) (MS)** • **Safety significant items (2) (Control room) (MS)** • **Safety significant items (3) (reactor auxiliary coolant systems) (MS)** • **Safety significant items (4) DC power systems (MS)**
Level 2 Prevention	Over pressure protection of coolant pressure boundary (MS)	Heat removal after reactor shutdown (MS) Safety shutdown functions outside control room (MS)	Emergency reactor shutdown (MS) Maintain sub-criticality (MS)	
Level 3 Mitigation	Containment of radioactive release [PCV] (MS)	Core cooling (MS) Mitigation of reactor pressure increase (MS)	Maintain sub-criticality (MS) Controlling power output increase (MS)	
Level 4 Accident Management	Radioactive release containment [reactor building, gas treatment] (MS) Severe accident management [PCV event] (MS)	Severe accident management [Make Up Water System, FP systems] (PS)	Severe accident Management (MS)	
Level 5 Accident Management				

Resilience: Extension of Defence-in-Depth

- Response to & Recover from the accident
- Preparation for the accident considering all phases (prevention, mitigation, response , recovery)