**Discussion of some new safety concepts and new safety requirements in light of the Fukushima nuclear accident**

CHAI Guohan, SUN Xuezhi, FENG Yi, FU Jie, LUAN Haiyang, DU Qian

( Nuclear and Radiation Safety Center, MEP, Beijing 100082, P.R.C)

**Abstract:：**After Fukushima nuclear accident, some new safety concepts and new safety requirements are suggested and discussed among the nuclear industry and nuclear safety regulatory organizations all over the world. In this paper, new safety concepts and new safety requirements, such as “Design Extension Condition”, “enhance the application of Defense-in-Depth”, “independence between different levels of Defense-in-Depth”, “enhance the diversity design of safety features”, “nuclear safety As High As Reasonable Achievable”, and “practically elimination of large release of radioactive materials” are discussed; and also it is stated in this paper that, with the consideration of “nuclear safety As High As Reasonable Achievable”, deterministic and probabilistic methodologies should be used to identify the safety vulnerabilities in the design of NPPs, and reasonable practicable measures should be taken to minimize the consequence of residual risk, and to achieve the safety goal of practically elimination of large release of radioactive materials.

**Key Words:** Defense-in-Depth; Practically elimination of large release of radioactive materials; Nuclear Safety As High As Reasonable Achievable; Design extension condition; Residual risk; Engineering safety systems; Additional safety system; Supplemental safety measures

1. **Introduction**

On 11 March 2011, a magnitude 9 earthquake that generated a series of large tsunami waves struck the east coast of Japan and caused severe damages to the Fukushima Dai-ichi Nuclear Power Plant (NPP), which led to hydrogen explosions at Unit 1, 3 and 4 in succession with massive release of radioactive materials. The Fukushima nuclear accident caused significant contamination to the NPP site as well as surrounding environment, and had serious impact on the confidence of the global community in nuclear safety and their acceptance of the nuclear energy and nuclear power, although the accident itself didn’t directly result in any human death.

The Fukushima nuclear accident is another catastrophe in human history of nuclear energy development. We should actively learn from the lessons, reflect on the safety of nuclear power, take suitable improvement measures for safety, and further enhance the safety level of nuclear power.

The most direct and profound lesson that we’ve drawn from the Fukushima nuclear accident is that severe accidents of NPPs are not as far away from us as we originally figured. We should pay enough attention to the severe accident condition in the NPP safety design, and place equal emphasis on the prevention and mitigation of NPP severe accidents. Moreover, previous study of NPP accidents mainly focused on internal events (including human factors); extreme external events, however, may cause many SSCs of NPP common cause failure, for which the Fukushima accident is an example. Therefore, it has to be resolved as safety issues regarding how to minimize the impact of external events on NPP safety and how to mitigate beyond-design-basis accidents caused by extreme external events (including severe accidents).

The Fukushima accident has brought grave consequences and profound lessons. Its occurrence precipitates re-examination and reflection on the understanding of nuclear safety and on the safety design of NPPs. It also manifests the importance of the defense-in-depth (DiD) philosophy, which has to be further enhanced in the design and operation of NPPs in the future. Meanwhile, the Fukushima nuclear accident demonstrates that it is not adequate enough for NPPs to only achieve the quantitative safety goals of the two “one-thousandth” as well as relevant probabilistic safety goal of CDF/LERF. The nuclear industry and nuclear safety regulatory authorities all over the world have carried out widespread safety examinations after the Fukushima accident, and started a large-scale debate on the new concept and new requirements of nuclear safety, during which the cliché of “How safety is safe enough” has once again become a hot topic.

1. **Lessons Learned from the Fukushima nuclear accident**

Compared with the Three Mile Island accident (USA 1979) and the Chernobyl accident (Ukrainian Republic of USSR 1986), the Fukushima Daiichi accident has some new features as followings:

(1) The direct cause that led to the nuclear accident at the Fukushima Dai-ichi NPP is the extreme external natural hazard. Both the Three Mile Island accident and the Chernobyl accident were caused by the internal events (including human error); and previous NPP safety analysis as well as studies on the prevention and mitigation measures for severe accidents were also mainly focused on initial internal events. The Fukushima nuclear accident warns us that the beyond-design-basis external events should be taken further consideration in the design and operation of NPPs.

(2) The earthquake and the induced tsunami resulted in complete station blackout (SBO) and loss of ultimate heat sink for long period of time in multiple units at Fukushima Dai-ichi NPP, which exceeded the original design of the NPP. In the traditional NPP design, it does not consider that accident would occur in more than one units at the same time, even if there’re multiple units at the site; in terms of station black out, it only assumes the loss of the off-site power and emergency diesel generator without consideration of loss of the DC power system, and it usually assumes that the power supply would be recovered within 1 to 3 days at the NPP site. However, during the Fukushima nuclear accident, not only did the NPP lose the AC power supply, but its DC power system, air compression system and illumination system all ultimately failed, hampering the ability of NPP operators to manage the plant conditions. The power supply had not been recovered for two weeks after the accident.

(3) No any instrumentation or control measures was available in the main control room (MCR) and some important onsite local place were inaccessible; the damage to the NPP system exceeded the coverage of Severe Accident Management Guidelines (SAMGs). Due to no control measures in the MCR, some mitigation measures could only be implemented on the local place; yet the earthquake, tsunami, hydrogen explosions and high temperature as well as high radiation level in certain place of the NPP greatly affected the emergency rescue and disaster fighting activities. The NPP system was seriously damaged which was beyond the coverage of SAMGs.

(4) The earthquake and tsunami caused great devastation to the NPP and the adjacent infrastructure. Rescue from the outside could not access in time while the emergency rescue and disaster fighting activities could not be implemented effectively. These all resulted in the continuous upgrades of the accident, and several units ended up with severe core damage one after another.

(5) Hydrogen explosions happened in unexpected location. The scene of successive hydrogen explosions in the Fukushima nuclear accident brought significant psychological impact to the public. In fact, the previous NPP design has already paid great attention to the control of hydrogen in order to prevent hydrogen explosion inside the containment vessel, which would result in the loss of last physical barrier for radiation release. But the hydrogen explosions in the Fukushima accident occurred outside the containment vessel, which indicates the deficiency of the human cognition on hydrogen behavior under severe accident condition.

(6) Actual emergency evacuation zone exceeded the emergency plan zone. Each NPP has set up an emergency evacuation zone for nuclear accident as the last barrier of the DiD system. The actual emergency evacuation zone in case of the Fukushima nuclear accident was 20km away from the site, exceeding that in the emergency plan.

(7) Large amount of radioactive waste water was produced. In the early stage of the Fukushima accident, large quantity of sea water and freshwater were injected into the reactor, containment vessels, reactor building and spent fuel pools for Unit 1 to 4; after the condition of the reactor cores and spent fuel pools of the Fukushima Dai-ichi NPP were gradually under control, there was large amount of radioactive waste water leakage in the plant, and how to handle it become an increasingly difficult issue. Three years after the accident, treatment of the large amount of radioactive water is still the most formidable issue for the Fukushima Dai-ichi NPP at present.

**3. Development of Safety Goals**

Fukushima Daiichi NPP was double stroked by strong earthquake and huge tsunami which caused severe nuclear accident and large release of radioactive materials, but Fukushima nuclear accident has not lead to the direct death of personnel, and is not likely to obviously increase the risks of cancer. The result shows that the safety level of Fukushima Daiichi NPP still satisfies the safety goals of the two “one-thousandth” (NRC suggested safety goals) for NPPs. That is, the risk to an average individual in the vicinity of a NPP of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the population are generally exposed, and the risk to the population in the area near a NPP of cancer fatalities that might result from NPP operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.). The Fukushima nuclear accident has further verified the safety of NPPs. However, Fukushima nuclear accident leads to great pollution and economic loss, the consequence of the accident is very serious. Therefore, Fukushima accident is not acceptable from this perspective.

Fukushima nuclear accident demonstrates that NPPs should also consider other negative consequences caused by nuclear accident, including the contaimination to environment, the panic of public and the instability of society, besides satisfying the safety requirement of two “one-thousandth”. Therefore, the Chinese government made a clear requirement on the *12th Five-Year Plan and 2020 Long-Term Goals on Nuclear Safety and Radioactive Pollution Prevention and Control* issued in 2012, that “the design of new reactors built in the 13th Five-Year period and afterwards should struggle to eliminate practically the possibility of large release of radioactive materials. Similarly, *Nuclear Safety Directive* amended by the Council of the European Union (EU) requests NPPs to avoid following two types of release: (1) early radioactive release, that would require off-site emergency measures but with insufficient time to implement them, (2) large radioactive release that would require protective measures that could not be limited in area or time. Besides, IAEA has started reviewing the amendment of *Convention on Nuclear Safety* suggested by Switzerland and other countries since early this year, which proposed similar requirements on nuclear safety.

The concept of “practically elimination” was initially brought up by European researchers, its purpose is to minimize off-site emergency response plan. *Safety of New NPP Designs* published by WENRA in March2013, pointed out that accident with core-melt which lead to early or large release have to be practically eliminated; for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures. Currently, European EPR design has adopted some measures which could practically eliminate those severe accidents scenario that might lead to the failure of the containment. However, there are a lot of debates on whether these measures are sufficient in post-Fukushima Era, whether they need to be further developed, and should mitigate or minimize the consequences of extreme accident condition (namely the residual risks) which exceeds the current human cognition.

The concept of “practically elimination of large release of radioactive materials”, on one side, is based on the political consideration to restore public confidence in the safety of NPPs after Fukushima nuclear accident; and on the other side, it sets higher goals for safety design of NPPs from technical and economic perspective, namely, within the scope of design basis accident (DBA) or design extension condition, nuclear accident will not lead to significant release of radioactive materials; under extreme severe conditions, large release of radioactive materials should be avoided, so as to protect people, society and the environment from the hazard of the radioactive material release, especially the hazard similar to the long-term, high-level contamination to the surrounding environment in Fukushima nuclear accident. The concept of “practically elimination of large release of radioactive materials” does not mean canceling off-site emergency plan, since the Fukushima accident has clearly manifested the importance of off-site emergency response. The meaning of “large release of radioactive materials” in the term “practically elimination of large release of radioactive materials” is different from large release frequency (LRF) in PSA level 2. To differentiate from the two, we may call LRF significant release of radioactive material, which might be more acceptable to the public; “Practically elimination of large release of radioactive materials” still uses “large”, similar to radioactive release of Fukushima nuclear accident.

Practically elimination of large release of radioactive materials considers the releases not only from core but also from other storage facilities such as spent fuel, the releases because of the severe accidents caused by both internal events and extreme external events either at early stages or at later stages and the gaseous emission to air as well as waste water discharge.

For severe accidents which challenge the integrity of containment, on the basis of additional safety systems to reduce the probability of its occurrence, deterministic approach and probabilistic approach as well as engineering judgment, may be used to demonstrate the integrity of the containment, such kind of analysis can be based on best estimate and realistic model.

**4. Innovation of Nuclear Safety Concept**

After Fukushima nuclear accident, international nuclear energy industry and many regulatory authorities carried out nuclear safety inspection, stress tests and capacity evaluation to cope with extreme external hazards. Based on the findings after inspection, analysis and evaluation, a series of improvement measurements aimed to improve the safety margin of NPPs and to enhance the ability to withstand the beyond-design basis external events was put forward and many new and higher safety requirements were developed for new NPPs.

**4.1 As High as Reasonably Achievable (AHARA)**

The three nuclear accidents in the history of nuclear power development fully demonstrates the properties of nuclear safety, which is that nuclear industry compared to other industries, possesses complexity of technology, sudden of accidents, difficulty for disposal, severity of consequences and sensitivity to social.

The lessons learnt from Fukushima nuclear accident once again informed us that due to the limitation of human cognition, there is potential uncertainty in nuclear power plant safety, i.e., residual risk to nuclear safety for NPPs. Regarding the extreme importance of nuclear safety, AHARA principle should be considered in nuclear safety design: that is to take all the reasonably feasible and practically effective measures to achieve higher nuclear safety level than that already meets the regulatory standards.

AHARA is derived from the concepts of ALARA (As Low as Reasonably Achievable) applied for radiation protection, as well as of ALARP (As Low as Reasonably Practicable) adopted by UK to control the risk of nuclear. And there is similar statement in para 2.2 of SSR-2/1 “to achieve the highest standards of safety that can be reasonably be achieved”.

AHARA principle will be the motive and foundation for sustainable improvement of nuclear safety in future. The application of AHARA will help enhance nuclear safety by adopting the up-to-date technology and research achievements, and assist the regulatory authorities as well as their TSOs promote nuclear safety more actively and improve regulatory requirements by summarizing nuclear safety improvement practices and experiences.

**4.2 Place Equal Emphasis on Three Aspects**

TTo absorb experience and lessons learned from Fukushima nuclear accident, we should place equal emphasis on three aspects in NPP designs:

1(1) Place equal emphasis on internal and external events. Compared with internal events, the attention paid to external events was relatively insufficient in the past. There is a lack of consideration on how NPPs could maintain safety when encountering beyond-design basis external events. In future NPP design and operation, we should pay more attention to events of small probabilities, making full consideration of and response actively to extreme natural hazards, strengthening resisting-measures on earthquake, flood, fire and air crash. For a range of selected beyond-design basis external events, they should be considered as design extension condition. Meanwhile, the capability of resisting beyond-design basis natural disasters can be enhanced by enlarge design safety margin, taking supplemental safety measures and strengthening defense in-depth. Besides, additional safety system and components dedicate for mitigating severe accidents should satisfy the requirements of functional available after SSE; so as to increase the survival probability of additional safety system and component under the condition of external events (e.g. the loss of off-site power due to earthquake and typhoon) plus other failures.

(2) Place equal emphasis on prevention and mitigation. The previous approach of dealing with severe accidents focuses more on prevention, especially the prevention of the occurrence of severe accidents. The major task of mitigating severe accidents is to prevent the failure of the containment; little consideration is given to the circumstances when there is a sign of challenge of the containment (e.g., when the actual pressure exceeds the design pressure). In future nuclear design and operation, more attention should be paid to the management of severe accident, and to ensure the independence between prevention and mitigation measures. As for selected severe accidents, which is considered as the design extension conditions, should use additional safety equipment which is different from engineering safety features to control the consequences of severe accident. As for the residual risks of NPPs, reasonable and practical measures should be taken to further reduce the probability and minimize the consequences of its occurrence, in order to achieve the goal of practically elimination of large radioactive materials. Mitigation measures should be taken for the filtered containment venting under extreme circumstances.

(3) Place equal emphasis on deterministic and probabilistic approaches. In the past, the requirement of nuclear design and safety analysis considered the deterministic approach as the major approach, while the probabilistic approach only serves as a supplement. In the future, we should enhance the DiD philosophy and the application of diversified designs, while strengthening risk-oriented decision making process, in order to maintain sufficient safety margin. We should also conduct full scope deterministic accident analysis and probabilistic safety analysis, and adopt methods including pressure test and safety margin analysis if necessary. Accident analysis should start with all kinds of normal operation conditions, until the condition of safety shut-down, so as to find out potential safety vulnerabilities as more as possible. Reasonable and practical safety measures should also be taken to further improve the nuclear safety level.

**4.3 Categories of plant states**

The suggested categories of NPP states is shown below:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Plant Design Envelop** | | | | |  | |
| Operation States | | Accident Conditions | | | | |
| Plant State | Normal Operation | Anticipated  Operation  Occurrences | Design  Basis Accident | Beyond-Design Basis Accidents | | | |
| Design Extension Condition | | | Residual  Risks |
|  | Severe Accidents | | |

The improving aspect is to identify the requirements of prevention and mitigation of design extension condition (including selected severe accidents), and to take relevant measures for residual risks.

**4.3.1 Design Extension Condition (DEC)**

The nuclear power industry of Europe has introduced the concept of design extension condition (DEC), which pays major consideration on a certain selected accident condition of beyond-design basis (including multiple failures and severe accident), and taking additional safety systems to cope with DEC. It also suggests appropriate acceptance criteria to DEC analysis results, and ensures the effectiveness of additional safety systems.

According to our understanding, the selected beyond-design basis accidents and selected severe accidents which were clearly identified Chinese in HAF 102-2004 *Safety Regulations of Nuclear Power Design* belong to DEC. However, we didn’t raise clear requirements on SSCs dedicated for coping with beyond-design basis accidents and selected severe accidents (existing SSCs for coping with design basis accident can be used to mitigate severe accident; and there is no specific requirements, such as seismic category and functional availability for SSCs specific designed for severe accident), and there is no clear acceptance criteria. This is mainly due to the reason that HAF102 didn’t raise fundamental requirements of safety design for the systems and equipment coping with selected beyond-design basis accident and selected severe accident. After the Fukushima accident, we need to raise clearly identified requirements for the prevention and mitigation of severe accident, and to extend the design condition of NPPs, introducing design extension condition, and to make specific requirement on its mitigation system and components.

DEC includes (1) selected multiple failure condition of NPPs SSCs, e.g. SBO, loss of ultimate heat sink, (2) selected severe accident, including corresponding severe accident phenomena, (3) selected extreme external events.

Additional safety systems should be used to cope with DEC, e.g. additional alternating power supply and water source, measures to avoid high-pressure core melt, measures to control hydrogen, measures of trapping and cooling molten core.

These additional safety systems should differ from engineering safety systems, and perform the defense-in-depth function of engineering safety feature. The key principle of the installation and design of additional safety system is no negative effect, so as to avoid the adverse influence on normal operation and the response function of anticipated operational occurrences (AOO) and DBA. Realistic and best estimate analysis method could be adopted to verify the effectiveness of the additional safety systems. The analysis result of DEC should comply with relevant acceptance criteria, e.g. the integrity of the containment.

**4.3.2 Residual Risks**

Residual risks refer to the beyond-design basis conditions which cannot be clearly identified or with very low probability of occurrence and with no effective measures of mitigation, such as NPP condition with extensive damage due to extreme external event. There are two types of residual risks: beyond the current human cognition; or the probability of occurrence is very low and there are no reasonable and practical coping measures.

Past nuclear design considers residual risks to be unimportant and did not consider coping measures. Fukushima accident indicates that residual risk should still be considered as important risks which cannot be neglected.

For residual risks, we could only reduce the consequence and achieve the minimum of it by enhancing safety margin and adopting supplemental safety measures and defense-in depth measures. The key principle of the installation and design of supplemental safety measures is to make sure that the nuclear safety to be as high as reasonable and practicable, and no negative effect. It is also recommended to make comprehensive consideration of the probability of occurrence and the risk elements of the consequences, and to avoid the adverse effects on normal operation and the response function of AOO, DBA and DEC.

**4.4 Safety Function and Safety Classification**

In understanding in the past, safety functions were normally limited to the scope of design basis accident conditions, that was, structure, system, components (SSCs) for protecting and mitigating design basis accident were required to implement safety functions. Fukushima accident demonstrates that, not only SSCs required for mitigating design basis accident to carry out fundamental safety functions of three aspects, but also SSCs for mitigating severe accident condition have to carry out fundamental safety functions of three aspects, Therefore, it is need to redefine safety function and safety classification.

In all operation condition, during or after design basis accident, and in the case of selected beyond-design-basis accidents condition (design extension condition), the fundamental safety function as follows must be implemented: (1) control of reactivity, (2) removal of heat from the reactor and from the fuel storage, and (3) confinement of radioactive material, control of planed radioactive release, and limitation of accidental radioactive release. In addition, in the design of NPPs, means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

The engineering safety systems used for mitigating DBA should maintain on safety class, which are the systems implementing safety function within range of DBA. The additional safety systems and supplemental safety measures for mitigating the beyond design bases accidents could be non safety class, but they should have some specific requirements, e.g. seismic category (available after SSE), availability ([equipment](javascript:void(0);) qualification), quality assurance, periodic test and so on. Besides, the active equipment used for implementing key safety function should take redundancy and diversity into account, such as pressure relief valve for serve accident, hydrogen recombiner and igniter.

**4.5 Extension and Promotion of application of Defense-in-Depth (DiD) philosophy**

As a fundamental principle of nuclear safety, defense-in-depth (DiD) philosophy is gradually formed, continued developed during the process of human using and developing nuclear power. The massive studies have proved that DiD concept play an important role to ensure nuclear safety. After Fukushima accident, nuclear industry have reflected and combed on DiD system, confirmed the importance of DiD philosophy for nuclear safety, and brought up the consideration for developing and improving application of DiD philosophy.

**4.5.1 Adjusted Defense-in-Depth System**

The suggested 5 level Defense in Depth system is shown below.

|  |  |  |  |
| --- | --- | --- | --- |
| Level of Defense-in-depth | Safety goals | Basic measures | Plant status |
| 1 | Prevention of abnormal operation and failure | Conservative design and high quality construction and operation | Normal operation |
| 2 | Control of abnormal operation and detection of failures | Control, limiting and protection system and other surveillance features | Anticipated operational occurrence |
| 3 | Control of accidents within design basis | Engineered safety features and Emergency operating procedures | Design basis accident（single failure initial event） |
| 4 | Control of serve accident, including prevention of serve accident（4a）and mitigation of consequence（4b） | Additional safety features and severe accident management | Design extension condition, including multiple failure（4a）,  severe accident（4b） |
| 5 | Emergency rescue work on extremely condition, mitigation of off-site consequence | Safety margins, Supplementary safety measures, DiD measures, Extensive damage mitigation, off-site emergency response | Residual risks |

The redefined DiD system, keeping the basic framework of the original five levels unchanged, and fourth level is subdivided into two parts to cope with DEC (with or without core melt), while strengthening the fifth level to cope with the residual risks.

The redefined DiD system divided safety SSCs as engineering safety features, additional safety systems and supplemental safety measures. The engineering safety features to cope with the design basis accidents, such as the Emergency Core Cooling System （ECCS）is safety class system, seismic I design, which requires conservative analysis to satisfy the safety requirement. Additional safety systems are specific designed to cope with the design extension conditions, such as severe accident rapid relief valves, could be non-safety class, but have to satisfy some specific requirements such as availability after safe shutdown earthquake, which needs realistic analysis to satisfy the safety requirements. supplemental safety measures are used to minimize the consequences of residual risk and the engineering rescue of extreme conditions, means the NPP equipped with mobile DG, mobile pump and reserved water for mitigating extensive damage state; mobile equipment of offsite assistant team; filtered containment venting measures, store and treatment features of radioactive waste liquid; and the safety storage building for mobile DG and mobile pump.

Engineering safety features and additional safety systems could perform similar safety functions, they could play roles as DiD. In the analysis of DBA, it is merely to consider the function of engineering safety features, not to consider the positive effect of additional safety systems. In the analysis of DEC, it is merely to consider the function of additional safety systems.

Under the redefined DiD system framework, the safety design of NPPs will strengthen the measures for the selected multiple failure conditions and selected severe accident condition, and take full account of sufficiency and reliability of the measures, achieve the balance reasonably between accident prevention and mitigation. At the same time with the principle of nuclear safety as high as reasonably achievable, the design should minimize the consequence of residual risk by enhancing the design safety margins, taking supplementary safety measures and DiD measures, preparing the EDMG and taking off-site emergency counter-measures, so as to practically eliminate of large release of radioactive materials.

**4.5.2 Enhance the Independence between the individual DiD Levels**

In previous NPP design, there were some problem of independence between the individual DiD levels, such as the equipment and safety system for design basis accident, they will also be used as possible in severe accident. If the system or equipment failure, the accident will break through multi levels of DiD.

After Fukushima nuclear accident, WENRA provided a technical view about the independence between the individual DiD levels in their report named *Safety of new NPP designs* released in 2013. The world nuclear power community and national regulatory authorities also have a lot of discussion about how to enhance the independence between the individual DiD levels, eliminate the dependent effect between different levels, in order to increase the effectiveness of different DiD levels and improve the safety of NPPs.

Therefore, in the design of NPP, all individual DiD levels should remain independent, and every subsystem in each level also should remain independent as possible. The design should focus on the independence of prevention and mitigation measures.

The requirements of independence between the individual DiD levels do not apply to passive barriers (such as containment). The requirements mainly for safety system and equipment which ensuring the integrity of barrier, that could improve the reliability of containment function.

**4.5.3 Extension of Application of DiD philosophy**

Previous design of NPPs did not consider extremely external events enough. The design ensure the conservative design basis for extremely external events, and take appropriate measures to ensure that design basis external event do not have effect on NPP safety. But it take less consideration on whether the NPP is safe and what measures could effective mitigate the consequence when NPP under the beyond-design basis external events. From the warning of Fukushima nuclear accident, because of the limitation of the human cognition and the uncertainty of analyze results, the designs of NPP need to have properly consideration about the consequence of NPP due to beyond design basis external events, which include: earthquake, flooding, fire, aircraft impact and so on. For the residual risks, the design should mitigate or minimize the consequence by enhancing safety margin, taking supplementary safety measures and DiD measures. The DiD philosophy is reflected in the document of *General Technical Requirements on post-Fukushima Nuclear Accident Improvement Measures for NPPs (tentative)* issued by the National Nuclear Safety Administration (NNSA) of China. Also for external flooding, DiD approaches could be taken to protect the NPP or minimize the consequence: the water-proof measures at NPP site level could protect NPP from the flooding higher than the design basis flood level (selected Beyond-Design Basis Accident, also called Design Extension Conditions), which will forbid water flooding in the reactor buildings; the water-proof measures in reactor building can help to reduce the influence areas once water flooding into the buildings; and the accidents management measures such as mobile DG and mobile pumps onsite and offsite can help to mitigate or minimize the consequence of extensive damage condition caused by flooding. This DiD mitigation strategy could promote the safety of NPPs, also control the costs of nuclear power construction and operation.

Appropriate DiD measures against extreme external events and NPP residual risks should be considered during NPP design.

**5. Innovation of Nuclear Safety Requirements**

After Fukushima accident, there were various opinions from different countries and experts on how to improve the safety of NPPs and how to practically eliminate large releases of radioactive material; however, what the meaning of “practically elemination” is, the most crucial point is how to translate it into nuclear safety requirements and NPP design practice.

China NNSA and its technical supporting organizations has organized to compile a document of *The Safety Requirements for New Nuclear Power Plants,* which would be issued in due time. More requirements related to practical elimination of large radioactive releases would be added in follow-up revision in the future.

Based on implementing the current nuclear safety regulations, *The Safety Requirements for New Nuclear Power Plants* complements and expends some key issues on nuclear safety, in which enhances the concepts of the diversification on design, and continuously improving nuclear power safety by using the most up-to-date technologies and research achievements.

**5.1 Safety Requirements for New NPPs**

**5.1.1 Safety Functions**

Clearly request that under the selected Beyond-Design Basis Accident conditions, three fundamental safety functions and after-accident monitor function must be implemented.

**5.1.2 Safety analysis**

The results of deterministic and probabilistic safety analysis must be considered.

PSA Level 1 and 2 on internal and external events during the plants states including power operation and outages must be fulfilled. The analysis objects include core, spent fuel poor, as well as other features containing a large amount of radioactive materials.

**5.1.3 Defense-in-Depth**

Emphasize the effectiveness of DiD and the independence between individual levels. DiD approach is also requested for defensing external events, especially through multi-level defenses to prevent and mitigate severe accidents caused by extreme external events.

**5.1.4 External Events Defense**

The site must forbid to settle in high seismicity areas and dangerous surface rupture zone cause by seismic activity. The areas where suppose to have over 0.3g limiting safety seismic motion are not suitable for siting, therefore it must choose in areas with low seismic activity. For new NPPs, the Design Basis Earthquake Motion Level （SSE）should not be lower than 0.30g; the earthquake warning system in NPPs should be able to initiate the reactor trip automatically.

The flood defense design of NPPs must consider the impact of extreme flood events and combined flood events. The NPP floor elevation should be higher than the design basis flood level.

For the NPPs with crash risk by large commercial airplanes, the design should consider the effects by large commercial airplanes crash.

**5.1.5 Station Black Out**

Besides the stationary additional power supply at the plant site, on a multi-units site at least two mobile DGs (one big and one small) and mobile pumps should be equipped.

The reliability of the offsite power should be enhanced, or appropriate compensatory measures should be considered.

**5.1.6 Safety Consideration on Severe Accidents**

Keep the concept of “beyond-design basis accident” (including severe accidents) in HAF102; however, to be consistent with the requirements by *IAEA SSR-2/1*, adopt the safety consideration for Design Extension Conditions in SSR-2/1.

**5.1.7 Severe Accidents Prevention and Mitigation**

Place equal emphasis on prevention and mitigation. Simultaneously, confirm to formulate and improve *The Severe Accidents Management Guideline*, covering conditions such as power operation, low power and shutdown states, and emergency responses to spent fuel pool and NPP extensive damage condition.

Measures such as responding station black out (emergency power supply), high-pressure core melt, global hydrogen explosion, molten-core concrete interaction, and containment bypass, etc. should be adopted in design.

**5.1.8 Reliability of the Ultimate Heat Sink**

Remove the residual heat from the safety important item of NPPs to the ultimate heat sink with high reliability in all plant operating modes; meanwhile the diversity of heat sink should be considered.

**5.2Follow-up Revision Consideration**

When upgrading the document of *The Safety Requirements for New Nuclear Power Plants,* the following items will be considered:

(1) Confirm the requirement of practically elimination large release.

(2) Promote the principle of nuclear safety As High As Reasonable Achievable (AHARA).

(3) Further reduce the Large Release Frequency (LRF), such as lower than 10-7.

(4) Adjust the categories of NPP states and the content of five-level DiD. Responding DEC condition in level 4, additional safety systems should be taken for mitigation. Responding the residual risks in level 5, measures including enhancing safety margins, complementary safety measures and DiD approaches, as well as off-site emergency intervention measure, should be carried out to minimize the consequences. Also the safety classification of SSCs dedicated for DEC mitigation should be confirmed.

(5) From the design point of view, the result of safety analysis for new NPPs should demonstrate that it is unnecessary for new built NPP to be equipped with the filtered containment venting system, and the necessity for off-site intervention measures to mitigate radiological consequences be limited or even eliminated in technical terms. However, considering the potential uncertainty in analysis results and the limitation of the human cognition, from the perspective of DiD, as a complementary safety measure, it is necessary to install filtered containment venting system. Thus, the release amount to the environment could be controlled by this fundamental measure, to ensure no long-term severe contamination by NPP accidents would happen in surrounding areas. In the meantime, off-site emergency preparedness and response by local government should be well prepared, but the containment filtered release should not be as a scenario of emergency response source term analysis. This off-site emergency preparedness and response plan could be minimized according to relevant laws and regulations.

The requirements of installing the filtered containment venting system or measure, not mean weaken design requirements, it is a supplementary safety measure which can strengthen the DiD. In the severe accident situation, although the probability of occurrence is not high, but there still exists some accident series that can cause the containment pressure exceed the design pressure. If the containment is in the situation of long term overpressure, the consequence maybe serious if the radioactive materials are discharged through uncontrolled containment leakage, it may cause serious contamination to the surrounding environment. To adopt filtered containment venting when necessary, and control the amount of release, is also a back up approach to remove the heat in the containment.

The requirements of installing the filtered containment venting system or measure, is also for harmonizing with the emergency requirements. This not only reflects the safety of NPP design, but also reflects the concept of DiD, make sure the scope of emergency protection action that actually carried out do not exceed the scope of emergency plan.

(6) From the design point of view, safety analysis should demonstrate that it is unnecessary for new built NPPs to be equipped with accident radioactive liquid waste storage facility. Considering the potential uncertainty in analysis results and limitation of the human cognition, from the DiD standpoint, it is necessary to install the radioactive liquid waste retention and treatment facilities. As supplementary safety measure, the facilities have the defense-in-depth measures and can avoid the radioactive liquid waste releasing to the environment. Regarding the radioactive liquid, as the last line measures, the four items that are storage, sealing, treatment and isolation need to be achieved in order to minimize the consequence of residual risk. The radioactive waste storage facility can be used as reservoir at ordinary times.

**6. Nuclear Safety Practice in China**

**6.1 ACPR1000**

Yangjiang unit 5 and unit 6 that have been approved by Chinese government after Fukushima accident are based on the big amount of under-construction and operation CPR1000, consider the experience feedback of Fukushima accident, apply the deterministic and probabilistic safety analyses methods, adopt reasonable and feasible improvement measures, such as：add Diversity Actuation System (DAS), add special instrument control cabinet for severe accident, adopt measures to guarantee the integrity of main pump shaft seal, add pressure relief valve dedicated to severe accident, add reactor vessel cavity water injection system, add one standby DG for each reactor, add one filtering device so that each reactor has its individual filtered containment venting system, add cooling tower as the diversity ultimate heat sink. All the above measures can enhance the capability of prevention and mitigation of severe accidents. ACPR1000 can satisfy the requirements of *Safety Regulations of Nuclear Power Design* (HAF102-2004), and reach the probability safety goals defined in the *12th Five-Year Plan and 2020 Long-term Goals on Nuclear Safety and Radioactive Pollution Prevention and Control* (Core damage frequency per reactor year should not exceed 1×10-5, large radioactive release frequency should not exceed1×10-6).

**6.2 CAP1400**

Through nuclear safety review and communication, and based on the consensus of utility, designer, and nuclear safety authority, CAP1400, which will be built in China, has made great safety improvements based on AP1000, such as: improve the seismic resistance of DAS system and adds earthquake automatic reactor trip signal, improve the seismic resistance of SSCs dedicated to mitigate severe accident consequence, improve the seismic resistance of standby DG in NPPs, improve the seismic resistance of igniter and add some PARs to control hydrogen in containment, enhance the seismic resistance of CCWS and SWS (which can transfer the residual heat into the sea, so that the sea can be the diversity ultimate heat sink), and perform the function as defense-in-depth, improve filtered containment venting measures, equipped with mobile DG and mobile pump. We believe that CAP1400 can satisfy the requirements of practically eliminating the possibility of large releases of radioactive materials.

**6.3 Hualong-1Reactor**

Chinese-designed Hualong-1 reactor type is based on the mature design and operation experience of million kilowatt reactors(M310), considering the experience feedback from Fukushima nuclear accident, fully considering the measures of preventing and mitigating severe accident, such as: equipped with double containments, equipped with sealing function for main coolant pump in case of pump shutdown, equipped with DAS system which is SSE seismic designed, a backup DG is equipped for each reactor, dedicated SSCs are equipped to cope with severe accident, adopt many diversity safety system design (active+passive), equipped with rapid pressure release valves during severe accident that can satisfy redundancy requirements, adopt IVR cooling function, equipped with filtered containment venting system, etc. The above measures have greatly improved the design safety level of NPPs.

**7. Summary**

Three severe accidents have been happened in the nuclear power history, each of them had caused profound influence to the development of nuclear power, and meanwhile, it had greatly pushed the updates of nuclear power technique and improvements of nuclear safety management, so as to achieve a higher phase of nuclear safety level.

The Chinese government has promoted nuclear safety to national safety strategic level, and proposed the Chinese nuclear safety concept which are rational, harmony and common, identified positive nuclear power developing policy in the premise of adopting international highest safety standards and ensure safety.

In order to promote the public confidence to nuclear power, achieve healthy, sustainable development of Chinese nuclear energy, the nuclear safety regulatory body and it’s TSOs have actively absorbed the lessons learned from Fukushima nuclear accident, carried out deep discussion and technical communication among international counterparts and nuclear industries in China, and launched massive exploration and practice about nuclear safety concepts and requirement innovation, such as:

1) Nuclear safety should be As High As Reasonable Achievable (AHARA).

2) The Design of NPP should be extended to DEC. Additional safety systems are needed in the NPP design to cope with the design extension condition.

3) The residual risk cannot be neglected. Plant states with extensive damage of SSCs caused by beyond design basis external event need to be considered. Design margin, supplement safety measure, and defense-in-depth measure should be considered to minimize the consequence of residual risk.

4) Practically elimination of large release of radioactive materials

5) Considering the nuclear safety As High As Reasonable Achievable, both deterministic and probabilistic safety analyses need to be adopted simultaneously during the design of NPP, identify the safety vulnerabilities probably exist in the design of NPP, and carry out reasonable and practicable measures to minimize the consequence of residual risk, so as to achieve the safety goal of practically elimination of large release of radioactive materials.