SAFETY AND STANDARDIZATION ISSUES ON ISO12100 OF SAFETY DESIGN AND OPERATION PRINCIPLE FOR NUCLEAR POWER PLANTS

MICHITSUGU MORI [1*]

[1] *Graduate School of Engineering, Hokkaido University*
kita13 Nishi8, Kita-ku, Sapporo, 060-8628 Japan
michitsugu.mori@eng.hokudai.ac.j

ABSTRACT

Huge tsunami in 2011 led the TEPCO Fukushima Dai-ichi NPPs into SBO and resulted in the core meltdown; meanwhile, three BWRs of Tohoku Electric Power Company, located most closely to the epicenter, could keep safe from any serious damages. PRA enables us to reveal the severity levels of systems to lead to SA and reasonably reduce the risk of CDF with the focused countermeasures; meanwhile, it must be required for the accountability on the residual risk in the irrecoverable accident even if the PRA shows much lower probability of CDF. ISO12100 of the safety design principle exhibits that the risk posed by the technology shall meet to preferentially perform the measures by technological design, and the accident prevention by the human management shall be expected as the decisive last resort. The evacuation plans should be established depending on the region and the season especially in the northern region with more detailed simulation including the effects of raining and snowing.

1. Introduction

Huge tsunami following the Pacific Ocean earthquake off the coast of the Tohoku region (the East Japan Great Earthquake) occurred on March 11, 2011, which led Tokyo Electric Power Company (TEPCO) Fukushima Dai-ichi (Number-1) nuclear power plants fallen into a loss of all external power, forced the units 1 to 3 into the core meltdown due to the station black out by losing all of the reactor core cooling functions except for the units 4 to 6 which were under the annual inspection. The all fuel bundles of the unit 4 were out from the core in the spent fuel pool, the flooding of which was maintained by the water injection from the outside reservoir and then by the recovery of the cooling function of the alternative facilities. The emergency diesel generators (DG, with air cooling) were equipped only for the units of 2, 4, and 6, and the one of unit 6 enabled to keep the reactor water level with water supply by the MUWC (make-up water system condensate) and led to the cold shutdown by a later recovery of external power supply, since it could escape from submerging of the related equipment and kept the sustainable state in operation. The unit 5 was also led to cold shutdown by the power interchanged from the unit 6.

TEPCO Fukushima Dai-ni (Number-2) nuclear power station had one single survived line out of all four external power lines and the water-cooled DGs were possible in operation at the unit 3 and 4. As a consequence, the reactor core isolation cooling system (RCIC) and MUWC through the accident management (AM) measures worked as the alternative water injection system and the residual heat removal system (RHR) by seawater-cooling, and then the all four units were successfully accomplished with the cold shutdown[1-2].

Tohoku Electric Power Onagawa nuclear power station is the closest to the epicenter. Despite the tsunami run-up height had reached to 13.8m, there is 14.8m land elevation of the ground height that was made with tough decision at the time when newly constructed. Although the circulating seawater pump motors were partially flooded, all of the units came to

* **Corresponding Author:** michitsugu.mori@eng.hokudai.ac.jp

be cold shutdown because one of the five external power supply lines could access to the electric power source and the water-cooled DGs of the units 1 to 3 were possible in operation [3]. In addition, the Onagawa Nuclear Power Station accepted about 240 refugees in the gymnasium of the Onagawa site from March 11th on the day of the earthquake. What factors had made the difference from such serious results? That should be traced for the nuclear power plants on the Pacific Ocean earthquake off the coast of the Tohoku region.

ISO12100 of the safety design principle exhibits that the risk posed by the technology shall meet to preferentially perform the measures by technological design, and the accident prevention by the human management shall be expected as the decisive last resort, meanwhile refraining from performing until the measures as much as possible to be considered by technology have been applied [4]. Hence, ISO12100 requires the inherently safe and fail-safe design measures for the design and production, and also requires the safety protection by the system and training in the organization for the users. Further, ISO12100 requires the introduction of the risk assessment which enable to reduce the risk and provide the benefits expected in manufacturers as well as in the users. The probabilistic risk assessment (PRA) is introducing in every country operating nuclear power plants. However, there exists the different aspect in the nuclear power from the industrial machinery. Even if the occurrence of failure or accident could show the much lower probability to lead to severe accidents, there needs the description on the residual risk for the neighboring residents and the public in the irrecoverable nuclear accident.

The new Nuclear Emergency Response Guideline requires the local government to prepare the evacuation plan before restarting the nuclear power plant. The Guideline specifies the zones and area to enhance the disaster prevention measures into three Emergency Planning Zones as PAZ (Precautionary Action Zone) within ~5km, UPZ (Urgent Protective Action Planning Zone) within ~30km, and PPA (Plume Protection Planning Area) within ~50km. However, as experienced in the Fukushima accident, the contaminated area will be different by raining and snowing as well as wind direction. There are 15 nuclear power plants including the under-construction plant in Tohoku and Hokkaido regions except for Fukushima prefecture. The evacuation plans should be established, depend on the region and the season especially in Tohoku and Hokkaido regions as a northern region with more detailed simulation including the effects of raining and snowing, the results of which are exhibited in the presentation.

2. Safety Concept Required for Nuclear Reactor Siting

The new Guidelines in the Nuclear Reactor Site Evaluation is outlined in “a. Principle Site Conditions”, “b. Fundamental Goals”, and “c. Guidelines for Site Evaluation” (the conditions for achieving the Fundamental Goals) by Nuclear Regulation Authority(NRA) of Japan. The each outline, a, b, c, contains the following three guidelines respectively [5].

a. Principle Site Conditions

a-1. No event to trigger Serious Accidents in the past and in the future, and to expand disasters.
a-2. The reactors are sufficiently distant from the public in combination with their safeguarding facilities.
a-3. The reactor site including the peripheral is in the environment which can take appropriate measures with respect to the public as required.

b. Fundamental Goals

b-1. Even if the occurrence of Serious Accidents is assumed in the worst case from the technical point of view in consideration of possible events surrounding the site, the reactor characteristics, and the safeguarding facilities (hereinafter referred to as "Serious Accidents"), the surrounding public never suffer the radiation damage.
b-2. Moreover, even if the occurrence of accidents, which exceed the Serious Accidents and cannot be considered to take place from the technical viewpoint, is hypothetically assumed, (hereinafter referred to as "Hypothetical Accidents": in which some of safeguarding facilities, which are expected to work effectively while the Serious Accident, are assumed not to work with the hypothetical dissipation of radioactive materials release equivalent to those in the Hypothetical Accident), the surrounding public never suffer the significant radiation damage.
b-3. The impact on the collective dose is sufficiently small in the case of the Hypothetical Accident.

c. Guidelines for Site Evaluation (the conditions for achieving the Fundamental Goals)

c-1. Establishment of a non-residential area around the reactor up to a certain distance and assurance that no one will live within that area in principle.

c-2. Establishment of a low population zone outside of the non-residential area such that the target radiation dose at the periphery of this low population density zone.

c-3. Still further, the reactor site is separated by a specified distance from the high density population zone.

These require the site area to be on the solid ground for building support from the viewpoint of earthquake resistance, the terrain to be in environment in which sufficient cooling water is obtained, and also to be away enough from the densely-populated residential area on the public exposure. The Regulatory Guide for Reviewing Nuclear Reactor Siting Evaluation and Application Criteria before the Fukushima accident also referred to the specified distance away from the nearby population. The safety design assessment should be required to perform in the Serious Accident through which the dissipation of released radioactive material is foreseeable under the worst scenario from a technological viewpoint, and also in the Hypothetical Accident which exceeds the Serious Accident level of radioactive material release though it could not consider to occur from the technological viewpoint. On the other hand, it was not explicitly guided in the new Guidelines for Site Evaluation by NRA that the following release rates of the amount accumulated in the core should be used 2% for Noble Gas, 1% for Iodine in the Serious Accident and 100% for Noble Gas and 50% for Iodine in the Hypothetical Accident as the source term in the event of loss of coolant accident (LOCA).

The issues also could be pointed out that the following exposure limits which was explicitly shown in the previous Guidelines for Site Evaluation by NRA are missing in the new one: the whole-body radiation dose of 0.25Sv or thyroid exposure dose (child) of 1.5Sv that must not be exceeded in the event of the Serious Accident on c-1; the whole-body radiation dose of 0.25Sv or thyroid exposure dose (adult) of 3Sv that must not be exceeded in the event of the Hypothetical Accident on c-2; the reference dose of 20,000 man-Sv as the limit on c-3[6].

3. Safety Design Concept for Nuclear Power Reactor

In order to avoid the external exposure by dissipation of released radioactive materials as described in the previous section, the nuclear power reactor is equipped with the reactor safety protection system, the reactor shutdown system to prevent undesired expansion of accidents, and the emergency core cooling system, reactor containment vessel, reactor containment spray system, and annulus air purification facility for the purpose of accident mitigation. Here is the idea of “Defence in Depth”. The word originally came from military meaning how the outbreak of the war or the occurrence of abnormality and accidents could be prevented, how their expansion could be prevented and the damage could be reduced. It is also used in non-military field such as the information security on the basis of the same idea. The term of “Multiple Protection” is sometimes used as Defence in Depth. However, both terms could not be exactly the same if the former is used in general as the series of multiplebarrier system. The each protection system should be independent from the others and never expect to keep their functions to be the backup for the others in Defence in Depth.

3.1 Defence in Depth

The definition of Defence in Depth is seen in TABLE 1 (LEVELS OF DEFENCE IN DEPTH) on 6 page of “DEFENCE IN DEPTH IN NUCLEAR SAFETY” of IAEA (INSAG-10) [7] by International Nuclear Safety Advisory Group (INSAG) and refer to the “SAFETY STANDARDS SERIES, SAFETY OF NUCLEAR POWER PLANTS DESIGN REQUIREMENTS, No. NS-R-1” [8]. The principle of Defence in Depth to be applied for the nuclear power reactor is described below as the five levels:

Level 1: Prevention of abnormal operation and failures

- ✔Fail safe/Foolproof
- ✔Interlock

✔protection against external and internal hazards (e.g. earthquakes, aircraft crashes)

Level 2: Control of abnormal operation and detection of failures

✔Reactor shutdown system

✔Reactor protection system

Level 3: Control of accidents within the design basis

✔ECCS

✔PCV

Level 4: Control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident

✔Feed & Breed

✔Filtered vent

Level 5: Mitigation of the radiological consequences of significant external releases of radioactive

✔Off-site response/ Evacuation

In Japan, the coverage of the multiple protection levels involved in the regulation was mainly the levels 1, 2, and 3. The level 4 was the voluntary-based safety of operators or utilities before the Fukushima accident. With regard to these levels 1 to 3 for the nuclear power reactor, there exist the so-called fivefold protection walls: ①fuel pellets (holding a radioactive substance generated inside the pellet); ②fuel cladding tube (external leakage prevention of radioactivity generated from fuel pellets); ③reactor pressure vessel/container (leakage prevention of radioactivity to mix into the coolant); ④reactor containment vessel (leakage prevention of radioactivity and radiation in case that the reactor pressure vessel is damaged); ⑤reactor building (leakage prevention to the external). However, the accidents inevitably might happen and it must have been considered that these functions at the accident could not work from the viewpoint of the safety consideration. These fivefold protection walls at safeguarding of the nuclear power reactor can increase only the reliability, but they must be considered to be nothing to do with the safety evaluation in the occurrence of the severe accident. Before the Fukushima accident, the nuclear power plants were said to be highly safe to prevent nuclear power plants from becoming severe accident because the fivefold protection walls corresponding to the levels 1 to 3 were working with high reliability, and therefore, the levels 4 and 5 were unfortunately not to be main concern and to be the voluntary-based safety issues of operators or utilities in Japan. After the Fukushima accident, it has been recognized that the security of consistency and the countermeasures to the severe accident to enhance the public protection must be necessary involving the regulation with the levels 4 and 5. The new regulation concept after Fukushima accident is shown in **Fig 1**, comparing with the conventional regulation. The countermeasures for severe accidents and counterterrorism are strengthened and newly required, especially for earthquake, tsunami, and the other natural disasters.

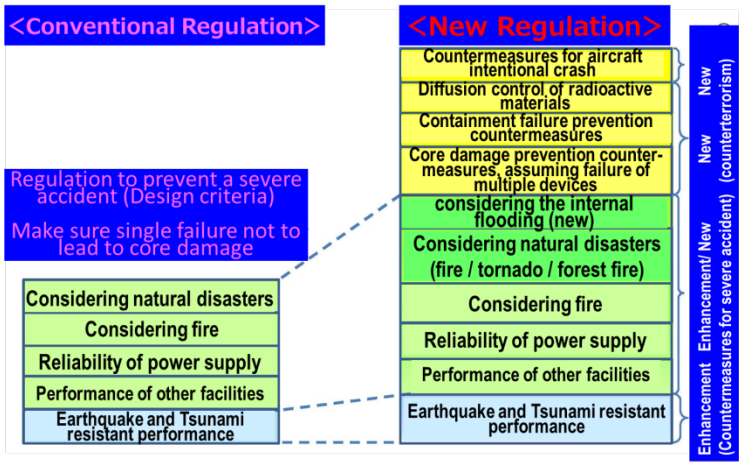

Fig 1. Concept of New regulation after Fukushima

3.2 Fail-safe and confirming the safety

Current reactors can reach the cold shutdown by “stop, cooling, and confining,” so that the safety is maintained. However, the loss of total power such a station blackout as occurred in the Fukushima accident shall impel the reactor to get out of control and into the core melting without any counter measures of cooling, on the process of which the protection system and

reactor shutdown system are designed to work as the fail-safe, but the reactor is eventually not the fail-safe design from the viewpoint to finally stop the reactor.

Shinkansen bullet trains can finally confirm the safety conditions by stopping as a last resort, discarding their functions of running same as other industrial machineries. On the contrary, the nuclear reactor which keeps generating the decay heat is unable to take such a way to confirm the conditions to be final safety by stopping as a last resort, and current large-output light water reactors (LWR) are never to be the fail-safe design. If the nuclear power generation should be counted as the main energy source again in the future, it must be provided with the intrinsically safer reactor than the current LWRs by fail-safe system, in which the safety and security could be acceptable for the public and especially residents near the nuclear power stations. There doesn't exist the absolute safety even if the fail-safe system is taken, considering the fact that unexpectedly occurs beyond the design basis. However, the possibility of realizing the safety is highly expected in the case that the fail-safe systems are going on in the operating system [9].

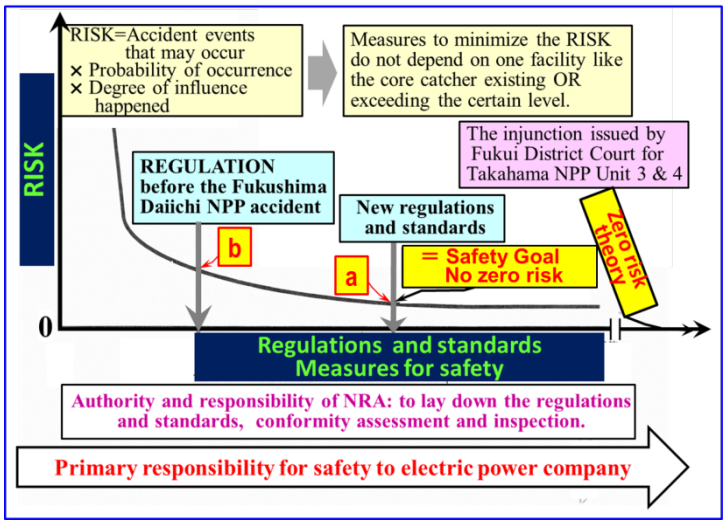

Fig 2. The concept of nuclear safety regulation

3.3 Issues on concept of the nuclear safety regulation

After the Fukushima accident, the new nuclear regulations and standards in Japan have tightened to reduce the risks especially against the earthquake, tsunami, and the other natural disasters. **Fig 2** shows the concept of the authority and responsibility of NRA in the nuclear safety regulation performance[10]. NRA has the commitment to lay down the regulations and standards, and to perform the conformity assessment and inspection. Assuming that the regulation level was tentatively at the point of **b** in **Fig 2** before the Fukushima accident, the new regulation level showed the reduced risk level as the point of **a** in **Fig 2** after the Fukushima accident. However, the risk will obviously be never to be zero as shown in **Fig 2**. NRA performs the conformity assessment whether the evaluated nuclear power plant can clear the new regulations and standards requiring the higher risk level than that shown at the point of **a**, in which there will be the residual risk lower than the point **a**. It should be considerably significant that the accountability for the remaining risk is redeemed.

On the contrary, the Fukui District Court issued an injunction to deny resuming operation of the Ooi nuclear power plant units 3 and 4 of the Kansai Electric Power Company (May 21, 2014) and the Takahama nuclear power plant units 3 and 4 (April 20, 2015) for the reasons to say that the probability of an accident is not zero; therefore, the basic human rights to life should be eroded once an accident occurs. This ruling is equal to say that it is not allowed to operate unless a state of the zero risk theory is realized, which corresponds to the far end of the horizontal axis shown in **Fig 2**. The state of zero risk can never be realized in real life and therefore it should be considered if the residual risk could be acceptable.

3.4 Issues on PRA for the acceptability of nuclear power plants

The probabilistic risk assessment (PRA) enables us to clarify the weaknesses of the equipment and system at a nuclear power plant and classify those level of severity to lead serious accidents. Therefore, it is possible to reasonably reduce the risk of core damage frequency with the focused maintenance depending on the level of severity for a serious accident leading to core meltdown. Nevertheless, PRA seems not to be actively applied for a nuclear power plant in Japan in contrast to the United States. It may still be considered that

the quantitative reliability should be enhanced and the effects of too much factors on PRA should be clarified. The new Nuclear Regulations and Standards revised after the Fukushima accident in Japan have tightened to reduce the risks especially against the earthquake, tsunami, and the other natural disasters with the deterministic countermeasures. There seems to exist the different aspect in them on the nuclear powers and also different from the industrial machinery. Even if the occurrence of failure or accident could show much lower probability to lead severe accidents, it must be required for the accountability on the residual risk in the irrecoverable accident in order to promote the nuclear power. ISO12100 of the safety design principle exhibits that the risk posed by the technology shall meet to preferentially perform the measures by technical design, and the accident prevention by the human management shall be expected as the decisive last resort.

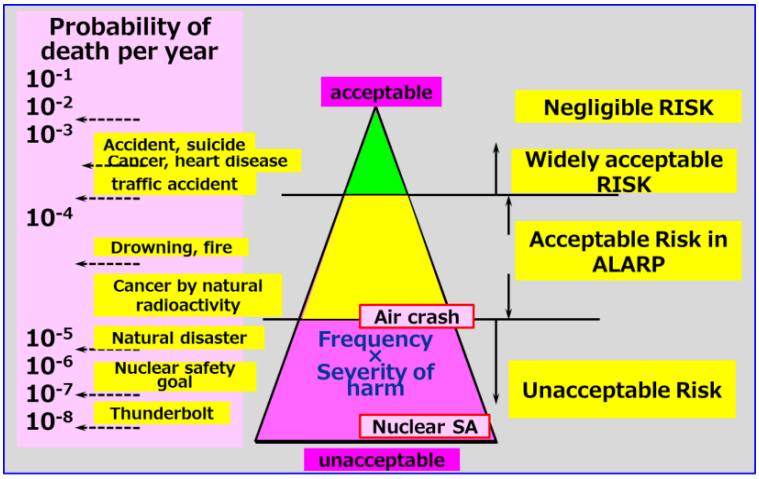

Fig 3. Probability of death per year and Principle of ALARP/ALARA

Fig 3 represents the concept of ALARP or ALARA and the fatal death probability per year due to risk initiating events. The acceptable risk is dependent on the magnitude of the product of the probability and damage, and the accident that would cause the irrecoverable serious results becomes unacceptable even if the product results have low probability. It is considered that the risk of the airplane accident is acceptable with the trade-off between the risk of the accident and the benefit for people who use it though the probability of an airplane crash accident leading to fatal is three orders of magnitude larger than that of a nuclear power plant. The acceptable degree of risk depends on the fields, conditions, and concept of the values of the various societies and different ages so that it is difficult to make a general decision.

Fig 4 shows the enhanced safety counter-measures for existing LWRs, some of which would work and keep their functions in the station blackout and enable to lead the nuclear reactor to cold shutdown. In these cases, the probability of the risk leading to the severe accident with core meltdown and remaining at the level of the point **a** in **Fig 2** would be extremely small. It may be acceptable for the people who reside far away from nuclear power plant and desire inexpensive electric power with stability supply by nuclear power plants. On the other hand, the Fukushima residents would hardly accept such risk, especially for those who experienced the severe accident and forced evacuation for long-term. It may still be the gambling for the Fukushima residents even the probability caused by tsunami or other natural disasters is so small.

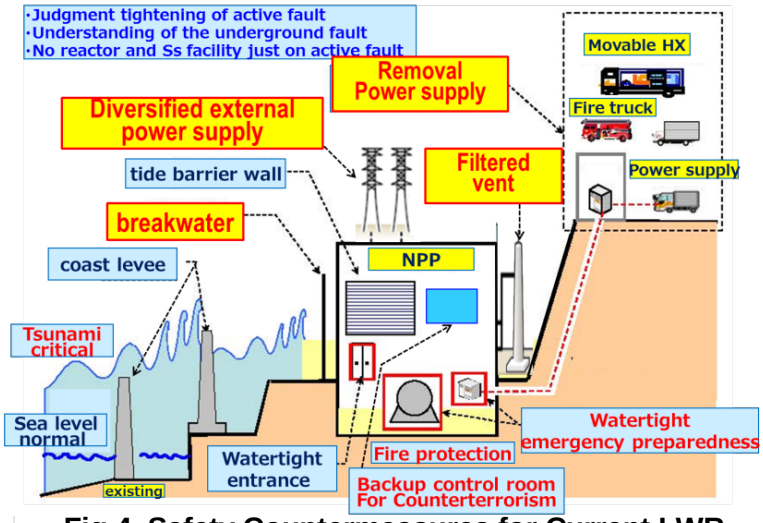

Fig 4. Safety Countermeasures for Current LWR against the new regulation after the Fukushima accident

4. New Evacuation Strategy for Further High Safety Concept

4.1 New Nuclear Emergency Response Guidelines

The new Nuclear Emergency Response Guidelines specifies the area to be focused and enhanced for the disaster prevention measures divided into three Emergency Planning Zones (EPZ), PAZ, UPZ, and PPA, as illustrated in **Fig 5** Conventionally, EPZ was defined as a range of area within 10 km from the commercial power reactors where the disaster prevention measures is enhanced. The revised disaster prevention measures are considered to enhance the level 5 in Defence in Depth. Hence, if the expansion of the accident disaster can be limited, e.g. within the site by the safety-enhanced nuclear power plants with the idea of the critical interlock as mentioned below, there is a possibility that "Frequency × Severity of harm" for nuclear accidents in **Fig 3** could be acceptable even for the Fukushima residents. Further, the UPZ within 30km expanded from the previous EPZ within 10km involves a greater number of people and local governments indiscriminately. It is necessary to drill them based on the feasible evacuation plan.

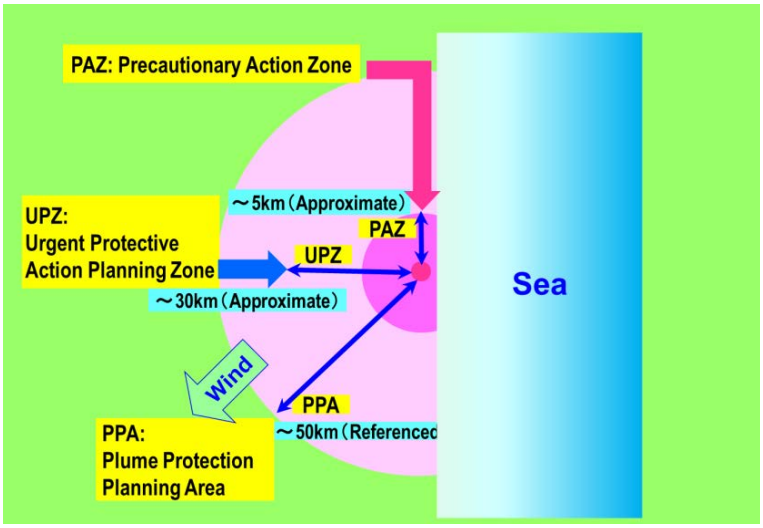

Fig 5. Areas to be focused and enhanced for the disaster prevention measures

4.2 Effects of seasons in northern region on evacuation planning

When fission products diffuse into the atmosphere, it is important to take protective measures such as evacuation after confirming actual weather conditions such as wind direction and speed, raining and especially snowing in the northern region. In fact such events, we meet the difficulty to obtain the adequate information and may not be able to fully respond to the situation. Considering such situations, it is considered much important to calculate in advance the atmospheric diffusion tendency of fission products taking account of the terrain and weather of the area before the accident occurs. Hence, the atmospheric diffusion analyses on fissions products from the source term were carried out using the atmospheric diffusion model for a northern region of snowy area. The deposition concentration were evaluated, depending on the distance from a nuclear power station based on annual weather.

Table 1 shows the analysis conditions for the concentration around the assumed source term located at the west coast facing the Japan sea in Hokkaido. The simulation was carried out with seasonal weather conditions under the assumption that small particles were released at the certain interval from the assumed source term. The results are exhibited as relative values in **Fig 6.** There are many mountains in Hokkaido, and many of the cities have the feature of being surrounded by mountain ranges. This leads to the thought to suppression of the diffusion of fission products, depending on the seasonal wind direction. In particular, in the case that the source term is between the mountain ranges, the incidence of deposits may be suppressed within the close-range area and the wet deposition may affect to accelerate. Differences were found from season to season. Particularly, the concentration distribution in winter shows different

Table 1. Analysis conditions for the concentration around the assumed source term

Analysis period	Jan. to Dec. 2014
Fission products release interval	60 minutes
Atmospheric Release	Unit Release
Number of released particles	200 pieces per discharge
Horizontal resolution	2.0km
Vertical resolution	400m

characteristics from other seasons, such as less deposition in the north-east direction and relatively large concentration distribution in the southeast mountain ranges. The evacuation plan should take into account the local geographical impact and the seasonal features, which are considered to be affected by the diffusion tendency having different atmospheric pressure arrangements depending on the season and the introduction of wet deposition process in consideration of the differences in precipitation substances.

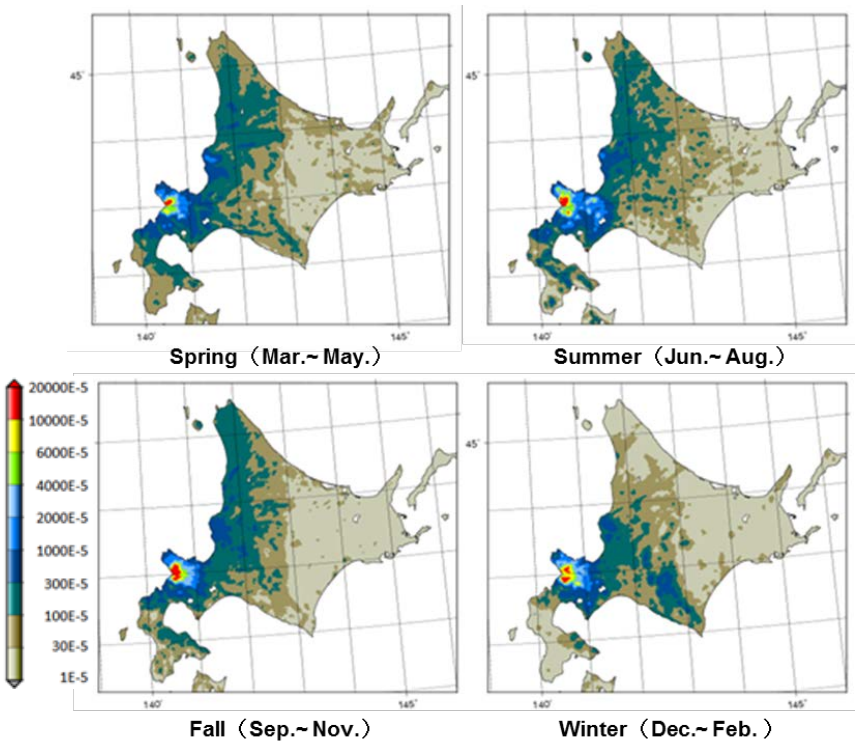

Fig 6. Effects of seasons in northern region

5. Safety Concept in Industrial Machinery and Nuclear Power Plant

5.1 Basic Concept of ISO12100

It is the world's standard in the safety design of machinery by ISO12100 that the risks accompanying with the machines should be reduced first by the design as much as possible. The safety must be confirmed to attain the certain safety level, but not allowed only by the image. As long as the risk can be foreseeable, the design must ensure the safety against the risk and it must not rely on users until all countermeasures by design be made. It is the last resort to expect the accident prevention by humans after applying all possible technical measures. If the vendor is unable to address the risks in terms of the difficulties in design and the cost evaluation, the vendor is obliged to tell and transfer the risks to the user. It should be noted to review if Japanese utilities and nuclear power machinery vendors had good communications allegedly before the Fukushima accident.

5.2 Comparison in Safety Systems of Nuclear Power and Industrial Machinery

If the performance and function at the time when they were designed and manufactured are maintained, the safety can be secured. However, the machine, which cannot be free from being deteriorated and worn, will be always considered to go wrong in the safety consideration. At that time, if equipment and devices can meet the fail-safe in the structure design, the structural maintenance can work to improve the availability factor. On the contrary, in the case that equipment and devices will work worse not to be fail-safe when their failures occur, the safety secure will depend heavily on the maintenance to keep their integrity, and further, the maintenance of quality is related to the safety [9]. No fatal accident has occurred on the super bullet train of Japan, Shinkansen, since the commercial service started. It can be said, therefore, that Shinkansen has kept 100% safe in the art. The safety concept of machinery such as Shinkansen takes the way to confirm the safety by stopping it at first as mentioned above, and then it is allowed to restart after removing the causes of troubles or accidents and having ensured the safety operation. On the contrary, the nuclear power plant can intrinsically never take the same way as Shinkansen's because the nuclear power plant keeps on generating decay heat and has to absolutely keep on operating to cool it without stopping.

Shinkansen can take the intrinsic safety system to stop same as the industrial machinery even in the case of total loss of power sources. Shinkansen's brakes are impelled to be free from the mechanical braking force by compressed air while running by electric power. Once the power to make the mechanical brakes free is turned off or lost, the mechanical braking system stops the train. That is, even if the loss of the entire power supply, Shinkansen can stop passively by the mechanical actuation.

The aircraft is unable to take the safety system by stopping while flying. Yet, the aircraft safety can be ensured after emergency landing and stopping except for air crashing, so that the aircraft safety could be heavily dependent on the accident management ability of the pilot operation before landing, the case of which should be supported as much as foreseeable in the design and manufacture.

5.3 Idea of elevating safety level

It is safety essential for the large facilities and plants that may cause the irretrievable disaster to keep taking the preventive steps and maintenance before the accident occurs rather than to take the corresponding recurrence prevention. Otherwise, if they are not intrinsically safe as the nuclear reactor due to the decay heat generation, the much-excessive requirements should be imposed on the maintenance to keep safe. The critical interlock shown in **Fig 7** [11] enables to prevent the machine from falling into the catastrophic situation to cause disasters. If it can be applied for the nuclear power plant, the nuclear reactor safety concept will be convincing. The critical interlock can be realized by the design that makes it possible to spontaneously stop the machine once its output level exceeds the preset critical point by physical phenomena as shown in **Fig 7**.

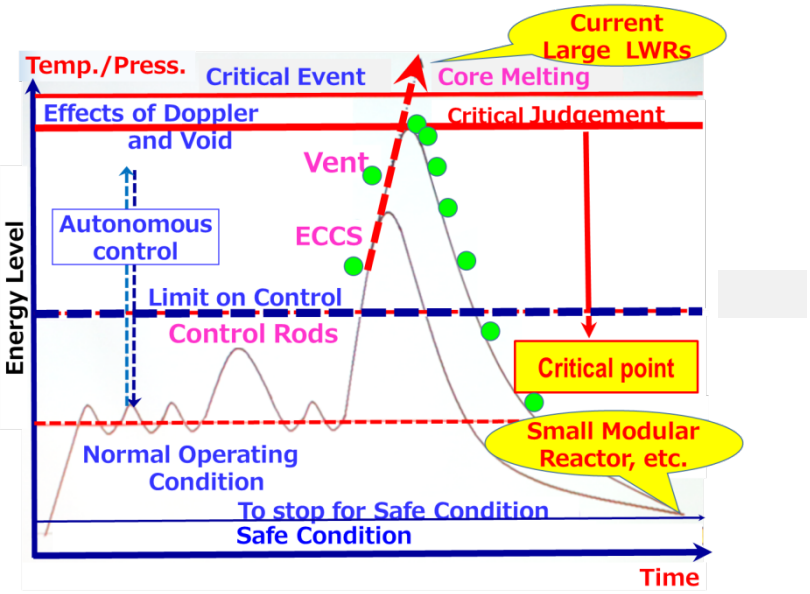

Fig 7. Concept of the critical interlock

It is extremely effective in the machine which can ensure the safety by stopping. It seems to be practically impossible to apply the idea of the critical interlock for nuclear power plants because the nuclear reactor cannot be secured safe even by scram to stop chain reaction of nuclear fission as mentioned above. The idea of the critical interlock in the nuclear power plant could apply for the case that, for example, it could limit the extent of disaster area within the plant site.

The nuclear power plant accident would bring the disaster irretrievable to the inhabitant in the large area around the plant as once caused in Fukushima. It must be deterministically controlled by initiating the critical interlock at the first stage of the accident before it comes into the uncontrolled state. Hence, the probabilistic risk assessment (PRA) is useful in considering the strategy of maintenance since the equipment and facilities in the plant can be classified from the viewpoint of their magnitude to impact the initiation of serious accidents. However, especially for the residents who were experienced with the nuclear disaster, the evaluation by PRA makes no sense even if PRA showed extremely low probabilities of accidents.

It must be first addressed in the design stage for the industrial machinery, assuming every condition to cause the accidents considered as much as possible. Nonetheless, it should rely on the human to finally stop it as long as the zero risk could not be attained as in **Fig 2**. It should be crucial and challenging to ensure the safety by the idea of the critical interlock

since it would come up against the compromise with the reduction of the output and economy.

6. Cost for Safety and Risk Reduction

There are valuable two cases to learn in considering the risk reduction and the required cost from the Great East Japan Earthquake, which caused enormous disaster by huge tsunami. One is the breakwater and floodgate whose height of 15.5m that saved Fudai-Village from ruin on the Sanriku-coast in the northern part of Iwate Prefecture [12]. Another is the Onagawa nuclear power station of Tohoku Electric Power Company which was attacked by the same huge tsunami which seriously damaged the Fukushima Dai-ichi nuclear power station. Nevertheless, the Onagawa nuclear power station could survive despite the fact that it is closer to the epicenter than damaged Fukushima one. The Onagawa nuclear power station was constructed with the tide breakwater whose height was 14.8m from the sea level (O.P.**:** Onagwa Peil) against the presumed tsunami as illustrated shown in **Fig 8** [13]**.** When the units 2 and 3 were newly constructed, the breakwater surface facing to the sea was reinforced by concrete, considering loss of ground soil by backwash. In addition, the seawater circulation pumps were installed inside the breakwater and then secured their functions without any serious damages. In the Fukushima Dai-ichi nuclear power station, all seawater circulation pumps were seriously washed away by tsunami and lost the cooling function. Tohoku Electric Power Company never eliminated the possibilities to cause unanticipated damages suffered from tsunami, and much of the cost spent for the land elevation and reinforcement work could reduce significantly the risk of serious damage at the severe accident. At the present Onagawa nuclear power site, the new breakwater with the height of 29m from the O.P. over the present tide breakwater is constructed as in **Fig 8**. The responsible attitude and ethics of the power company to continuously pursue to override the defined criteria of safety design could have escaped from fatal destruction of Tohoku district as well as company himself.

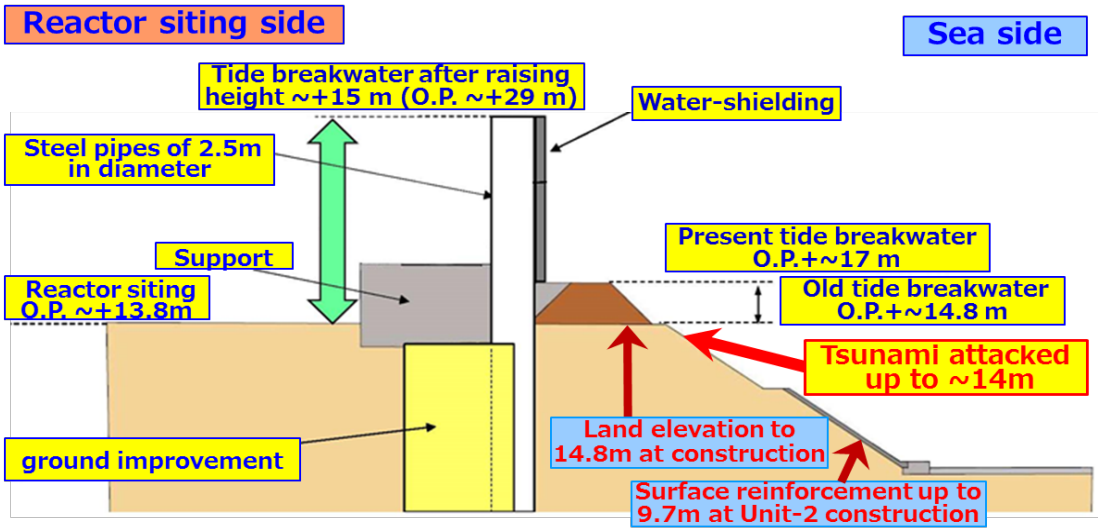

Fig 8. Onagawa nuclear power site land elevation and reinforcement against tsunami

7. Concluding Remarks

Discussions were made on the issues of safety and standardization about severe accidents of nuclear power plants. There exist points in the new guideline which shall be explained clearly in more detail for the remaining risk with the accountability.

The UPZ within 30km expanded from the previous EPZ within 10km shall involve a greater number of people residing and local governments indiscriminately. It is necessary to drill them based on the well-designed evacuation plan, which should take into account the local geographical impact and the seasonal features.

PRA is valid and useful in planning the strategy of maintenance since the equipment and facilities of the plant are classified based on their importance related to the initiation of accidents. On the contrary, it seems especially true for the inhabitant who experienced the nuclear disaster that the evaluation by PRA hardly makes sense without the accountability for the residual risk even if PRA showed extremely low probabilities of accidents.

The nuclear reactor which generates the decay heat is unable to confirm to be finally safe by stopping as a last resort. It is extremely difficult to simply attain the fail-safe requirements.
,
The concept of the critical interlock enables to prevent the machine from falling into the catastrophic situation to cause disasters. If it can be applied for the nuclear power plant, the nuclear reactor safety concept will be convincing. It should be crucial and challenging to ensure the safety by the critical interlock since it would come up against the compromise between the reductions of the output and economy.

It should be learned from the case that Tohoku Electric Power Company never eliminated the possibilities to cause unanticipated damages suffered from huge tsunami, and much of the cost spent for the land elevation and reinforcement work could have reduced much of the risk of serious damage. The corporate social responsibility and ethics beyond the determined criteria continuously pursued by the company saved the Tohoku district from fatal destruction and the company himself.

References

[1] Nuclear and Industrial Safety Agency, “Overview of the accident of Tokyo Electric Power Company Fukushima Dai-ichi nuclear power station”, Nov., March, 2011

[2] Tokyo Electric Power Company, “Actions in Fukushima Dai-ichi and Dai-ni nuclear power station”, June, 2012.

[3] Tohoku Electric Power Company, “Investigation Report on the tsunami caused by the Pacific Ocean earthquake off the coast of the Tohoku region at the Onagawa nuclear power station”, July, 2012

[4] ISO12100-1:2003, Safety of machinery －Basic concepts, general

[5] Nuclear Safety Commission, “Guidelines in Reactor Site Evaluation and its guide on application and Assessment.” May, 1965 (partly revised), March, 1989

[6] http://www.nsr.go.jp/data/000050240.pdf

[7] International Nuclear Safety Advisory Group(INSAG), “DEFENCE IN DEPTH IN NUCLEAR SAFETY”, INSAG- 10, IAEA, Vienna, 1996

[8] IAEA, “SAFETY STANDARDS SERIES, SAFETY OF NUCLEAR POWER PLANTS: DESIGN REQUIREMENTS, No. NS-R-1”, Vienna, 2000

[9] Masao Mukaidono, “Useful Safety Science”, Plant Engineer, Feb. 21, 2011, pp.49-50

[10] The 21st Century Public Policy Institute, paperback No.47, 2015

[11] Keita Honma, Noboru Sugimoto, “The concept of defense in depth and critical interlock of nuclear power plant”, Safety Engineering Symposium, 2013, pp,338-341

[12] http://www.nikkei.com/article/DGXNASFK31023_R30C11A3000000/

[13] Tohoku Energy Conference, Monthly magazine,”Hiroba”, No.451, August 2015