Efforts to Continuously Improve Safety of Japan's PWR Plants

YASUSHI NAGATA[*1] MAHIRO YAMAGAMI[*2]
FUTOSHI TANAKA[*3] YASUSHI TAKAYAMA[*4]
MASANOBU NAKANO[*5] AYAKO TAKEUCHI[*5]

To continuously improve the safety of Japan's nuclear power plant that were restarted after the Fukushima Daiichi Accident, Mitsubishi Heavy Industries Ltd. (MHI) has been continuously working on the voluntary improvement of the safety of nuclear reactor facilities together with electric power companies. MHI has been performing Probabilistic Risk Assessment and Stress Test for nuclear reactor facilities, deriving measures to further improve safety while developing technologies for new facilities to realize these measures. This report introduces examples of these efforts. MHI will continue to make a unified effort together with the electric power companies to continuously improve the safety of nuclear reactor facilities.

1. Introduction

In nuclear reactor facilities, voluntary safety measures had been implemented before the Fukushima Daiichi Accident. Since the Fukushima Daiichi Accident, emergency safety measures have been implemented based on the lessons learned from the accident, measures against severe accidents according to the new regulation and other measures to improve safety. As a result, 16 units in Japan's nuclear reactor facilities (as of August 11, 2020) have obtained permission for amendment of the reactor installment license for restart. Since the nuclear reactor facilities were restarted, further safety improvement efforts such as incorporating overseas insights have been continuously implemented. Some examples of MHI's efforts to support the voluntary activities of these electric power companies are described hereafter.

2. Efforts to continuous safety improvement

2.1 Activities toward continuous safety improvement

In nuclear reactor facilities, safety improvement has been promoted with measures against severe accidents based on the new regulation and subsequently, further safety improvement measures have been achieved through the installation of specialized safety facility, etc.

The assessment for improvement of the safety of nuclear reactor facilities introduced in this report (hereinafter referred to as the Safety Improvement Assessment) is a system in which electric power companies carries out under the legislation, a periodic and comprehensive safety assessment for all of the restarted nuclear reactor facilities. After carrying out a periodic inspection of each nuclear reactor facility, electric power companies are requested by the regulatory authority to carry out the Safety Improvement Assessment, report the assessment results to the Nuclear Regulation Authority and publicize them.

The Safety Improvement Assessment must be continuously improved. The "Operational

*1 Deputy Director, Nuclear Plant Designing Department, Nuclear Energy Systems, Mitsubishi Heavy Industries, Ltd.
*2 Chief Staff Manager, Light Water Reactor Service Project Department, Nuclear Energy Systems, Mitsubishi Heavy Industries, Ltd.
*3 Chief Staff Manager, Reactor Core & Safety Engineering Department, Nuclear Energy Systems, Mitsubishi Heavy Industries, Ltd.
*4 Chief Staff Manager, Nuclear Plant Designing Department, Nuclear Energy Systems, Mitsubishi Heavy Industries, Ltd.
*5 Chief Staff Manager, Advanced Plant Safety Department, Nuclear Energy Systems, Mitsubishi Heavy Industries, Ltd.

Guide for the Periodic Safety Assessment of Continuous Improvement of Commercial Nuclear Reactors”(1) (hereinafter referred to as the Operational Guide) stipulates that, in principle, the “assessments of implementation status of activities for safety improvement” (Probabilistic Risk Assessment (hereinafter referred to as PRA), Stress Test, etc.) shall be revised every 5 years, and the “medium- to long-term assessments of implementation status of activities for safety improvement” shall be revised every 10 years.

It also stipulates that the report shall specifically describe strengths and weaknesses in terms of the safety of nuclear reactor facilities and also describe short-term and medium- to long-term course of actions for safety improvement, as well as plans regarding specific measures for safety improvements. Electric power companies have been continuous working on safety improvements, based on their short-term, medium-term and long-term safety improvement plans.

With the periodic reporting system described above, the Safety Improvement Assessment is intended to achieve spiral-up of continuous safety improvement. (**Figure 1**)

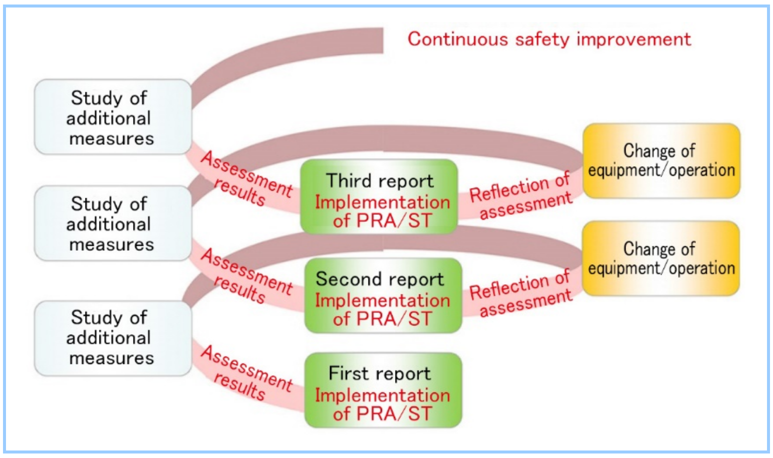

Figure 1 Image of continuous safety improvement

2.2 MHI’s efforts

MHI, as a nuclear power plant manufacturer, comprehensively conducts basic design to installation work/test and post-operation maintenance/inspection of component units of nuclear reactor facilities, and has accumulated enormous amounts of operating data about operations and failures of Japan’s and overseas nuclear reactor facilities. Using this experience and knowledge, we provide technical support on PRA and the Stress Test, of which the electric power companies must carry out by themselves as part of the Safety Improvement Assessment.

In addition, MHI, together with electric power companies, has been continuously making efforts to contribute to the spiral-up of safety improvement at nuclear reactor facilities by examining measures based on the Safety Improvement Assessment results, supplying equipment required for installation and conducting plant modification. Furthermore, we have been endeavoring to continuously advance and develop safety assessment methods, for example, by developing a systematic methodology to evaluate the effects of natural hazards that have uncertainty (earthquakes, tsunamis, etc.) and introducing the latest overseas PRA insights.

Each method of PRA and Stress Test will be described in chapter 3 and some of the measures for safety improvement derived from the assessments will be described in chapter 4.

3. Methods for safety assessments implemented in Safety Improvement Assessment

This chapter describes the methods for PRA and the Stress Test we have conducted.

3.1 Probabilistic Risk Assessment (PRA)

In PRA in the Safety Improvement Assessment, focusing on accidents that may occur at nuclear reactor facilities, a series of events (accident sequences) that lead to core damage or containment failure are comprehensively examined and the occurrence frequency of the accident sequences are quantified. PRA provides not only insights about an accident sequences and their frequencies, but also insights useful for improving the safety of nuclear reactor facilities, such as the relatively vulnerable aspects in nuclear reactor facilities and quantitative information of the effectiveness of safety measures. These PRA insights are obtained through analysis of the effects and contribution of the reliability of equipment and operator actions on the accident frequencies.

The Operational Guide, it is stated that PRA of internal events and external events shall be performed. MHI has been conducting the following assessments at the time when the Safety Improvement Assessment results for each nuclear reactor facility must be reported to the Nuclear Regulation Authority.

(1) Internal events PRA

Internal events PRA is conducted for events resulting from internal causes such as random failures of the equipment in nuclear reactor facilities and human errors by operators or maintenance workers. In the assessment, all events that challenges the normal operation of nuclear reactor facilities (initiating events) are identified, and subsequent scenarios that may lead to severe accidents (accident scenario) are analyzed and the frequency of the occurrence of severe accidents is quantified.

In the identification of initiating events, we investigate existing at Japan's and overseas PRA studies and also conduct detailed analysis to search for any cause in each system that may challenge normal operation of and trigger a initiating event.

In accident scenario analysis, we identify the safety functions required to mitigate each selected initiating event and then comprehensively develop accident sequences using the Event Tree method. In a PRA, 30 or more initiating events are modeled and a total of several hundred accident sequences are identified. In the process of the accident scenario analysis, we determine the minimum number of equipment and the operating time, required to achieve safety functions for each accident scenario. These conditions are called success criteria. The success criteria are set based on the analysis results of the thermal-hydraulic analysis code that simulates the behavior of nuclear reactor facilities during an accident.

In addition, in assessing the reliability of safety functions, we use the Fault Tree method by which models all combination of events that lead to the loss of the safety function. The fault tree considers events such as random failures of equipment and human errors of operators or maintenance workers. In the fault tree, equipment failures and human errors that may cause the loss of functionality of each system associated with safety functions are depicted in a tree-like logic diagram. MHI has developed PRAs with fault trees modeling more than total of 10,000 equipment failure events or human error events.

Concerning equipment failures, the Bayesian estimation approach (Bayesian updating) is used to reflect the plant specific operational experience obtained from the nuclear reactor facility on the generic component failure rates, which is estimated from the operational experience obtained from nationwide nuclear reactor facilities. The plant specific failure rates of components are assessed using by Bayesian updating. Regarding human errors, the information obtained from the operation manual for the nuclear reactor facility to be assessed, interviews with operators, and the allowable time for operation obtained from the thermal-hydraulic analysis simulating the nuclear reactor facility are used to quantify the probability of human errors specific to the nuclear reactor facility. To quantify the probability of human errors, we use the software for Human Reliability Analysis (hereinafter referred to as HRA), HRA Calculator, developed by the EPRI (Electric Power Research Institute) of the U.S.

Thus, we develop a systematic model (PRA model), which is an integration of the above assessments, and quantify the core damage frequency or containment failure frequency resulting from internal events.

(2) Seismic PRA (external event)

Seismic PRA is conducted for accident scenarios resulting from damage to structures, systems and components (hereinafter referred to as SSCs) caused by earthquakes.

In seismic PRA, the accident scenarios that are not within scope of internal events PRA, for example, the scenario where wide-ranging equipment in the nuclear reactor facility are simultaneously damaged by earthquakes, are also analyzed. In addition to the collection of information related to the assessment, plant walkdowns by PRA analysts and design experts are also conducted to check and gather information of the installation status and management status of the facility.

To calculate the core damage frequency or containment failure frequency, we use a seismic PRA model in which site-specific seismic hazard information, probability of damage to SSCs according to the seismicity (seismic fragility) and accident scenarios specific to earthquakes are taken into account.

The site-specific seismic hazard information is assessed by the electric power company and presented to MHI. Regarding the seismic fragility of various equipment, the insights from seismic designs are used to assess the actual seismic resistance/response distributions and the probability of damage to SSCs according to the seismicity is calculated.

We build a seismic PRA model, based on the PRA model for internal events, by adding accident scenarios specific to earthquakes and taking into account the seismic fragility of SSCs and the human error probabilities under seismic conditions. In the assessment, it is essential to appropriately understand and interpret the seismic design and system design, as well as the PRA technique. Integrated and comprehensive knowledge of the plant design is required to conduct the assessment.

(3) Tsunami PRA (external event)

Tsunami PRA is conducted for accident scenarios resulting from damage to SSCs caused by tsunamis.

In tsunami PRA, the accident scenarios that are not within scope of internal events PRA, for example, the scenario where wide-ranging equipment in the nuclear reactor facility are simultaneously damaged by the tsunami, are also analyzed. As with seismic PRA, plant walkdowns are also conducted in addition to the collection of information related to the assessment.

To calculate the core damage frequency or containment failure frequency, we use a PRA model (tsunami PRA model) in which site-specific tsunami hazard information, probability of damage to SSCs according to the height of the tsunami (tsunami fragility) and accident scenarios specific to tsunamis are taken into consideration. In particular, for the assessment of tsunami fragility, we have taken the lead in developing a new method(2) for providing the damage probability as a function of the height of the tsunami, and applied the method to fragility assessments of actual equipment for the first time in the world. In the new method, the uncertainty factors of actual equipment robustness and response, driven by the characteristics of the tsunami, such as flooding, submergence or wave power, are taken into account.

By performing a PRA, we can obtain not only information about core damage frequency and containment failure frequency, but also quantitative information about how and what types of accident sequences, equipment failures, equipment damage or human errors affect the frequency of severe accidents. Based on the information thus obtained through PRA, we derive measures to effectively reduce the risk from severe accidents.

The Operational Guide specifies that the events to be assessed in the Safety Improvement Assessment shall be increased in stages according to the maturity of PRA methods. The guide also specifies that the latest Japan’s and overseas insights shall be incorporated in the PRA. In other words, it is required for the Safety Improvement Assessment that the latest insights and methodologies related to PRA should be continuously investigated and when a new methodology has become practical, it should be incorporated in PRA or events within the scope of the PRA should be increased.

To this end, electric power companies have been making efforts to improve PRA by holding review meetings of pilot plant PRAs with experts invited from other countries. State of the practice PRA technology and insights are obtained through the review meetings. These efforts were started in 2017 and a total of five review meetings focusing on the following events were held:

- Internal events during at-power operation
- Internal events during shutdown
- Seismic events
- Internal events focusing on accidents leading to containment failure

MHI has been promoting the improvement of PRA methods in cooperation with electric power companies, through review meetings with overseas experts (**Figure 2**), analyzing the insights and observations indicated by the experts and addressing the findings. Through these efforts, we received comments from the overseas experts on areas that need further improvement, and also obtained information about the state of the practice PRAs in the U.S. and Europe. Based on the latest knowledge thus obtained, we have continued the development of PRA-related technologies toward the establishment of the world standard PRA in Japan.

Figure 2 Review meeting with overseas experts

3.2 Stress Test

In the Stress Test, on the assumption that a beyond-design-basis external event (earthquakes, tsunamis, etc.) occurs, the safety margin of a target nuclear reactor facility is evaluated by investigating to what degree the target nuclear reactor facility can withstand the event without significant damage to the core and spent fuel and without containment failure, as well as no abnormal emission of radioactive substances, and a cliff edge (limiting point) is identified to clarify the potential relative fragility of equipment.

The cliff edge is identified as follows: first, based on the results of seismic and tsunami PRAs, the initiating events (loss of off-site power, loss of component cooling water system, etc.) that may damage the fuel assemblies, etc., are selected. For each initiating event, the functions required to mitigate the impact of the event are extracted, an event tree is created, and then a scenario to terminate the progress of the event is identified. Next, the equipment directly related to each of the selected initiating events and the equipment related to the mitigation functions are extracted, the margin of each equipment against earthquakes and tsunamis (with the parameters of "seismic acceleration" and "height of tsunami") is assessed. Finally, a cliff edge is obtained. As an example, the seismic evaluation is described below.

The seismic acceleration at which each initiating event occurs is identified based on the seismic acceleration at which the equipment function is lost, resulting in the initiating event. The seismic acceleration at which an mitigation function is lost is identified based on the seismic accelerations at which equipment functions included in the mitigation functions in the event tree for each initiating event are lost and a smaller value is identified as the seismic acceleration at which an mitigation function is lost. Among the mitigation functions included in each event convergence scenario, the lowest seismic acceleration at which the function is lost is identified as the seismic acceleration at which the function is lost in the safe shut down scenario. If any one of the relevant mitigation functions is lost, the safe shut down scenario does not hold. Therefore, the lowest value is selected in each safe shut down scenario. Finally, among the safe shut down scenarios, the safe shut down scenario in which the seismic acceleration at which the function is lost is highest is identified as a cliff edge scenario and the seismic acceleration at which the function is lost in the safe shut down scenario is identified as a cliff edge seismic acceleration.

This assessment method was established as an assessment method applicable to Japan's nuclear reactor facilities with reference to the "Assessment Procedures and Implementation Plan Regarding the Comprehensive Assessments for the Safety of Existing Reactor Facilities Taking into Account the Fukushima Daiichi Accident of Tokyo Electric Power Holdings Co. Inc."(3) instructed by the Nuclear and Industrial Safety Agency, Stress Tests in Europe, etc. Since then, we have been conducting assessments similar to PRA concerning individual earthquake and tsunami events and assessments concerning the superposition of earthquakes and tsunamis and events associated with earthquakes and tsunamis which are specific to the Stress Test, at the time when the

Safety Improvement Assessment results for each nuclear reactor facility must be reported. Assessments concerning the superposition of earthquakes and tsunamis and events associated with earthquakes and tsunamis which are specific to the Stress Test are described below.

(1) Seismic induced tsunamis

Whether buildings, equipment, etc., are damaged or lose functionality when a beyond-design-basis earthquake and a subsequent beyond-design-basis tsunami occur is assessed based on the insights from seismic and tsunami PRAs. In this assessment, the seismic acceleration parameter and the tsunami height parameter are treated as independent parameters and every combination of both parameters is taken into consideration.

(2) Seismic induced event and tsunami induced events

Cliff edges in the event of an earthquake or a tsunami are identified based on the locational condition of nuclear reactor facilities and with consideration given to the equipment featuring functions that can be expected to prevent or mitigate events induced by earthquakes and tsunamis (internal flooding, fires inside or outside buildings, etc.) that may cause the cliff edges. This assessment is conducted to verify that the seismic safety margin alone or tsunami safety margin are not affected (the cliff edge is not lowered) by seismic induced flood, s by seismic induced fires or tsunami induced fires.

4. Measures for continuous safety improvement of nuclear reactor facilities

4.1 Measures for safety improvement

Through analysis of the effects of the equipment and operational reliability on the occurrence of accident sequences and the identification of cliff edges based on safety assessments, the potential and the relative fragility of the equipment can be clarified. If we can derive measures that may resolve the relative fragility, we can assess the degree of the measures effect and reflect the results in the safety activities of electric power companies and equipment modification work for nuclear reactor facilities toward the further improvement of safety.

Measures derived from PRA and the Stress Test vary by nuclear reactor facilities and include various scales of measures, such as short-term and medium-to long term measures. Some examples are as follows:

- Upgrading (improvement of seismic capacity) the metal-clad switchgear (on-site power system)
  Components inside the metal-clad switchgear are reinforced or replaced and its enclosure is reinforced so that the functional capacity against seismic induced vibration is improved.
- Automatic switching of recirculation
  The water source for the emergency core cooling system is switched from tank outside the reactor containment facility to a sump at its bottom on the inside. Related valves and pumps are remotely operated to reuse the water stored in the sump. The series of operations are automatized to realize a quick and reliable switchover.
- Shutdown seal for the primary coolant pump (Reactor Coolant Pump, hereinafter referred to as RCP)
  With this seal, the leakage of reactor coolant from RCP sealing portions (hereinafter referred to as RCP seal LOCA) is prevented for a long time. This measure is described more specifically in the following section.

The implementation of these measures is decided by electric power companies that operate the nuclear reactor facilities based on their judgement toward the further improvement of safety. MHI supplies equipment and carries out the modification work required for the implementation of these measures.

Among the aforementioned measures, the RCP shutdown seal is described.

4.2 RCP Shutdown Seal

In nuclear reactor facilities, the core is cooled by reactor coolant and reactor coolant must be stored. In a pressurized water reactor (hereinafter referred to as PWR), one of the facilities that make up the pressure boundary to store the reactor coolant is an RCP. RCP shaft sealing portions are cooled during normal operation and maintained under low-temperature conditions, so that the soundness is maintained. When a station blackout (hereinafter referred to as SBO), etc., occurs, the seal cooling function is lost and the sealing portions are exposed to high-temperature and high-pressure conditions. If these conditions continue for a long time, the sealing performance cannot be maintained. As a result, an RCP seal LOCA may occur.

When such conditions occur, the RCP Shutdown Seal is activated and prevents an RCP seal LOCA for a long time. The RCP Shutdown Seal is installed in the RCP sealing portions and it is composed of a sealing portion and a driving source. If the sealing portion is exposed to high-temperature and high-pressure conditions, the driving source is activated to bring the sealing portion into contact with the main shaft of RCP, so that the leakage of RCP is restrained. (**Figure 3**)

Application of this equipment allows securement of reactor coolant in the case of events such as SBO and the "cooling" and "confining" functions of nuclear reactor facilities, which are important for maintenance of safety, are also enhanced, leading to further improvement of the safety of nuclear reactor facilities.

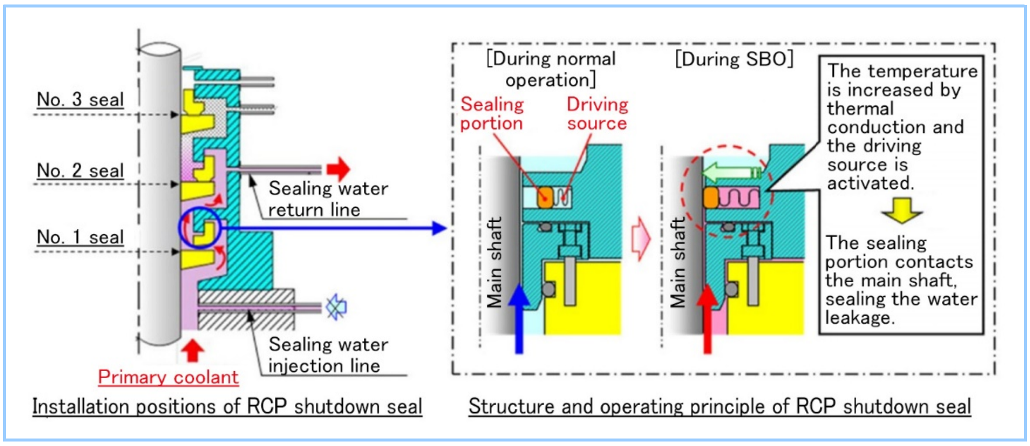

Figure 3 Outline of RCP shutdown seal

5. Conclusion

MHI will continuously contribute to the improvement of the safety of Japan's PWR plants through the assessment of the strength and vulnerability of nuclear reactor facilities using PRA and Stress Test based on the technologies we have developed so far, as well as through the proposition and development of measures to reduce the risk of severe accidents. We will also enhance our PRA by expanding the scope of the PRA and increasing detailedness of the PRA, through expert review and incorporating successful Japan's and overseas studies. Furthermore, we will study measures for safety improvement, develop technologies and equipment required to realize the measures and make proposals to our customer electric power companies in a timely manner so that they can be incorporated, thereby strongly assist the electric power companies' activity to enhance the safety of nuclear reactor facilities.

References

(1) Operational Guide for the Periodic Safety Assessment of Continuous Improvement of Commercial Nuclear Reactors, Nuclear Regulation Authority, (2017)

(2) R.Haraguchi, et al., Development of a fragility evaluation methodology for the Tsunami PRA, ASRAM2017, No.1052, 2017

(3) Assessment Procedures and Implementation Plan Regarding the Comprehensive Assessments for the Safety of Existing Reactor Facilities Taking into Account the Fukushima Daiichi Nuclear Power Station Accident of Tokyo Electric Power Holdings Co. Inc., Nuclear and Industrial Safety Agency, (2011)