17th International Conference on Probabilistic Safety Assessment and Management &
Asian Symposium on Risk Assessment and Management (PSAM17&ASRAM2024)
7-11 October, 2024, Sendai International Center, Sendai, Miyagi, Japan

Proposal of a method for developing a plant response model considering the effects of an impact with a time lag during the progress of an accident

Eishiro Higo*, Tsuyoshi Uchida
Central Research Institute of Electric Power Industry, Yokosuka, Japan

Abstract: Probabilistic Risk Assessments (PRAs) have been developed to identify vulnerabilities of nuclear power plants (NPPs) to events that disrupt normal operating conditions. Many conventional PRAs assume that internal events or hazards will challenge plants at the beginning of an accident. However, the Fukushima Daiichi NPP accident in 2011 has reminded us that hazards could affect plant response with time lag. The sequence of the accident, which was initiated due to the earthquake-induced loss of off-site power and reactor scram, was drastically exacerbated by the tsunami, which arrived about 40 minutes later. Conventional PRAs do not assume the situation where additional hazards affect the plant in the middle of the accident sequences, and do not incorporate the time difference of multiple impacts into the plant response model.

This study proposes a method to develop a plant response model that considers the effects of an impact with a time lag during accident progress based on the timeline of accident sequences through the development of an "event progression scenario diagram". This study first generalizes the scenarios in which multiple impacts with different arrival timings affect the plant response, and the possible situations are organized. Based on the organized scenarios, we illustrate an event progression scenario diagram by organizing information on the time of the accident sequence. We identify the system affected by the impact by comparing the timing of the event progression and the additional hazard. The proposed method is illustrated with reference to a typical event progression timeline. Since the proposed method can be easily applied to conventional PRAs and the applicable scenarios are of a general nature, it is expected to be used in a wide range of areas, such as combined hazard PRAs and multi-unit PRAs.

Keywords: Combined-hazard PRA, Seismic-tsunami superposition PRA, Accident sequence analysis, Time lag.

1. INTRODUCTION

A probabilistic risk assessment (PRA) is a tool for identifying the vulnerability of nuclear power plants (NPPs) to accident initiators. As PRA technology has matured, PRAs for various hazards have been implemented and refined; however, conventional PRAs for the hazards deal only with a single hazard.

The Fukushima Daiichi NPP accident has reminded us that additional hazards occurring in the middle of the accident progression can affect the plant response. The sequence of the accident, from the earthquake-induced loss of off-site power and reactor scram, was drastically exacerbated by the tsunami, which arrived about 40 minutes later. Identifying vulnerabilities due to the combined hazard of earthquakes and tsunamis is important for Japanese utilities.

One of the characteristics specific to the combined hazards is the time lag between the earthquake and tsunami arrivals on an NPP [1]. The effects of tsunamis disturbing the mitigation functions of an earthquake-induced initiating event may lead to new scenarios that have not been considered in conventional single-hazard PRAs. Moreover, depending on the time lag between the arrival of the earthquake and tsunami hazards, variations in scenarios (e.g., variations of mitigation measures affected by the hazard) may occur. Each of those scenarios may have different structures, systems, and components (SSCs) to which a tsunami damages. However, conventional PRAs do not assume the situation where additional hazards affect the plant in the middle of the accident sequences, and yet no method can incorporate the time difference of multiple impacts into the plant response model used in conventional PRAs.

This study proposes a method for developing a plant response model that takes into account the effects of additional hazards with a time lag during accident sequences. We show how to identify the mitigation functions that can be affected by the additional hazards by organizing the timeline information of the accident sequences through the development of event progression scenario diagrams.

In Section 2, we first generalize the scenarios in which multiple hazards with different arrival times affect the plant response and organize the possible situations. Based on the organized scenarios, we identify the elements that should be reflected in the plant response model. Then, Section 3 shows the proposing method identifying the mitigation functions affected by the additional hazard, by organizing information on the time of the accident sequence to create an 'event progression scenario diagram' and compare the timing of the event progression and the additional hazards. In Section 4, the proposed method is illustrated by reference to a typical event progression timeline. Section 5 concludes the study and shows possible applications.

2. CLASSIFICATION OF SITUATIONS IN WHICH TWO HAZARDS AFFECT A PLANT

To understand the characteristics of the situations where additional hazards affect the accident progression after an initial hazard induces an initiating event. We illustrate the situation with several generalized elements. The generalized patterns of the situations are categorized based on the combinations of initial and additional hazards.

2.1. Elements of the Situation in Which Two Hazards Affect a Plant

Let us consider what patterns can exist when accident mitigation functions are affected by additional hazards after an initiating event has occurred. The situation can be schematized as a combination of three elements: the affected plant, the initial hazard, and the additional hazard. Since the affected plant itself remains the same in any pattern, the distinctions among patterns are based on the sources of the two hazards and their relationship (see Figure 1).

The first group of cases is when multiple hazards with a time lag reach the plant. This pattern can be seen in the context of combined-hazard PRA. According to a study, hazard combinations can be categorized into the following three groups: independent (coincidental) events, correlated events, and consequential events [2]. Independent events mean no relation exists between the hazards. An example is external flooding and independent internal fire. When hazards share common factors and are correlated in their occurrence, the combination is called correlated events. An example is high air temperature and biological flotsam. The last category is the consequential events. The hazards are in a consequential relationship where one hazard causes the other one. A typical example is the earthquake and tsunami combination.

Second, the cases in which a single hazard affects a plant two or more times are considered. These situations can arise when we extend a single hazard PRA by considering multiple shocks or multiple modes. The first pattern is a situation where a hazard may strike a plant more than once. Using an earthquake as an example, this is the case where the plant is affected by aftershocks during operating mitigation functions for the accident progression induced by the main shock. Another pattern in which a single hazard affects multiple times can be a case in which multiple types of impacts have time differences in their arrival. For example, under a tsunami hazard reaching a site, pulling waves and pushing waves can reach the plant with their respective peaks at different time points.

Other possible effects may be due to cascading effects at sites where multiple units are located. In multi-unit PRA, from the view of the affected unit side, the additional impact from other units can be treated as a kind of additional hazard with a time lag, though the impacts among units are interactive. For example, the effects of a hydrogen explosion occurring in an adjacent unit may affect the unit before core damage. For a more detailed discussion on the types of multi-unit interactions in PRA, see the report for multi-unit PRA [3, 4].

Toward detailed hazard analysis and fragility analysis for the combinations of the initial and additional hazards, the categories should change the results depending on their correlations due to common factors or consequential relationships among hazards. Once we have obtained the information on how often the hazards occur and how much probability each component can be damaged, these multiple patterns do not change the fact that the plant response is affected by these hazards with time lags in accident sequence analysis, and it does not matter what is causing the effects. Identification of affected SSCs and estimation of SSC damage probabilities allows the model to reflect the effects of additional hazards.

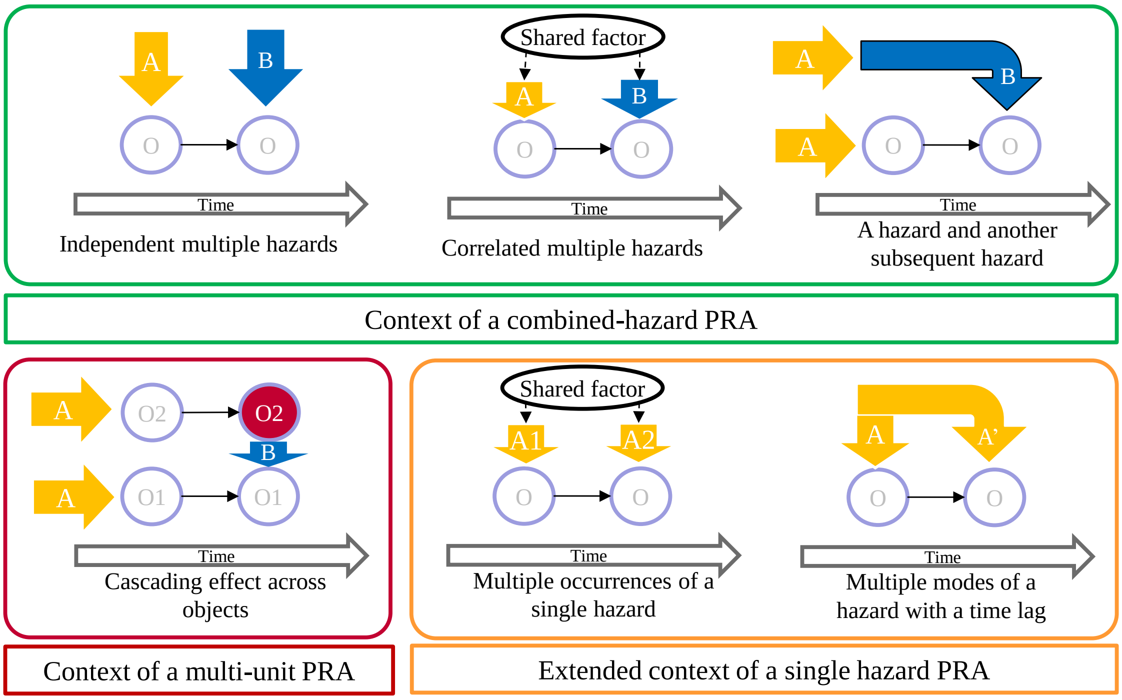


Figure 1. Categories of Situations in Which Two Hazards Affect a Plant

2.2. Effects of Time Lag Between Hazards

To identify what can happen when an additional hazard affects a plant in the middle of the accident sequence, we compare the case where the initial and the additional hazards reach “simultaneously” with the case where the additional hazard reaches “in the middle” of the accident sequence. The following effects can be considered as major differences from the case of acting at the same time:

- The mitigation function acts until the additional hazard stops functioning, thus mitigating the accident progression compared to the case of loss of function at the same time as the initiating event.
- The longer time required to complete alerts for additional hazards and the preparation of the workplace environment after the hazard arrives, the latter time to provide mitigation functions.
- There is no need to consider the simultaneous action of multiple external stresses on the SSC.

The influence of a mitigation function against accident progression until the additional hazard disables the functionality may differentiate the accident sequence analysis from the analysis ignoring the positive aspects of the interrupted function. First, if there are mitigation functions that complete the functionalities before the additional hazards reach them, the additional hazards cannot disturb the functions. Note whether additional hazards may disrupt the continuation of completed functions.

Second, the success criteria may change. For example, if the influence of the mitigation function until it is damaged by the additional hazard is significant, we may be able to add some systems that have been assumed that their functions are not enough for accident mitigation into the lineup of mitigation. However, this idea is inconsistent with the conventional PRA, which sets a mission time for each mitigation function and treats all failures to meet it as a uniform failure of the function, so it needs to be consistent with the single hazard PRAs.

A similar influence to the change of success criteria exists in relaxing a margin time for mitigation functions. The increased margin time to complete the preparation of severe accident measures may reduce the human error probability.

On the other hand, for mitigation functions that require tasks local workplace the time to alert for additional hazards and to prepare the workplace environment after reaching the site may be longer, which may delay the time to start the function.

Other possible aspects may be eliminating the need to consider the case where external stresses due to multiple hazards act simultaneously in the fragility assessment of the SSC, which is expected to reduce the risk compared to the case where they act simultaneously.

This study proposes a modeling method that focuses on the first explained point: “If there are mitigation measures that complete the functions before the additional hazards reach them, the effect of the additional hazards on those functions can be ignored”.

3. PROPOSING METHOD

To reflect the influence of the time lag of the additional hazard on a plant response, we propose a method how to identify mitigation functions that would be affected by the additional hazard.

3.1. Basic Concept

We assume that the initiating event is caused by a hazard that first reaches the plant, and additional hazards then affect the plant during the subsequent accident response. The accident sequence after the initiating event is assumed to be representable by the mitigation system event tree (ET) corresponding to the initiating event, and the impact of additional hazards is assumed to be representable by the reliability model (FT), calculating the success or failure probability of ET branches.[1]

Depending on the arrival time of the additional hazard, the SSC affected by that hazard may vary. Each of those scenarios may have different SSCs to which a tsunami damages. Mitigation functions that successfully complete the function before the additional hazard arrival are not affected by the hazard. We propose a method to identify those SSCs.

3.2. Procedure

For mitigation functions that are expected to be completed between the initiating event and the arrival of the additional hazard, as long as the completed functions are not affected by the additional hazard, it is not necessary to consider the effects of the additional hazard.

To identify mitigation functions and events affected by additional hazards, it is necessary to organize the relationship between the hazard impact arrival time and the operating time of each mitigation function.
We organize information on the time of mitigation functions in the accident sequence and extract event progression scenario diagrams.

Step 1. Make a list of mitigation functions.

We first generate a list of expected mitigations and possible consequential events for the targeted initiating event. This should be equivalent to a list of headings in the event tree of mitigation systems.

Step 2. Information gathering and estimation of the operating period of mitigation functions.

---

[1] If the impact of the additional hazard cannot be expressed only in terms of loss of mitigation function (reflected in the FT), in order to express it as a scenario, such scenario needs to be considered as an initiating event by decomposing it on the ET. When considering such initiating events, we should be aware that the timing of the effect of the additional hazard is considered to be almost simultaneous with the occurrence of the initiating event.

For each mitigation function and consequential event, we need to gather information to estimate the times shown below:

- Time of occurrence of a consequential event (e.g., Reactor coolant pump (RCP) seal LOCA)
- Startup time of the mitigation function
    - Timing of startup signal
    - Temperature and pressure curves until the conditions necessary for operation switchover
- Preparation completion time of countermeasures against severe accident, etc. (function startup time)
- Function completion time of mitigation functions and countermeasures against a severe accident, etc. (function startup time + mission time)

Note that the estimation of the preparation completion time for severe accident countermeasures should be done with caution. If outdoor on-site operations are required for the preparation of countermeasures against a severe accident, the effect of the timing of additional hazard arrival should be reflected at the stage of organizing this information.

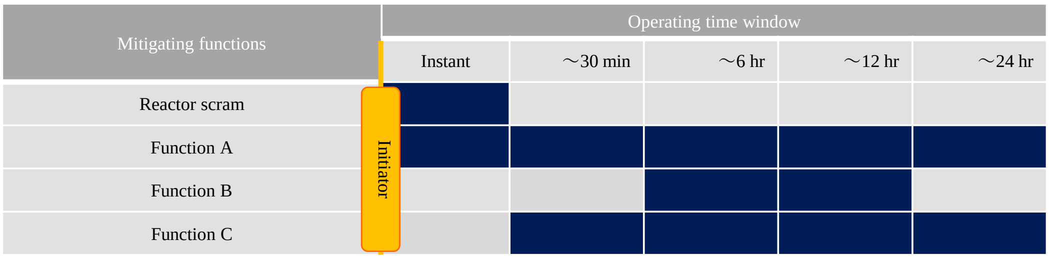
After an initiating event, it may not be possible to restore outdoor access routes and start preparation for operations in an environment where additional hazards are expected to arrive. Therefore, the delay in the arrival time of additional hazards delays the start time of mitigation operations. Therefore, for a given mitigation operation time, the following relationship needs to be satisfied

$$X > A + B + C, \tag{1}$$

where “A” denotes the time from the occurrence of the event to the time when outdoor work can be started; “B” refers to the time required to secure the access route; “C” represents the time required to prepare for mitigation operations; and “X” denotes the time required to successfully complete the mitigation operations.

Step 3. Draw timelines within which systems function.

Next, using the information, event progression scenario diagrams are created based on the mitigation system ET. Each mitigation function and consequential event considered in the mitigation system ET is lined up on the vertical axis, and the time of operation or the time of occurrence of the event is plotted on the horizontal axis. The mitigation functions that are required in parallel or subordinate to an event progression scenario are arranged in successive rows to form a block, and the core damage state or PDS to which the scenario leads is described at the end. This procedure allows us to draw an event progression scenario diagram that clearly shows the operating time of each mitigation function (see Figure 2).



Mitigating functions	Operating time window				
	Instant	～30 min	～6 hr	～12 hr	～24 hr
Reactor scram	■				
Function A	■	■	■	■	■
Function B			■	■	
Function C		■	■	■	■

Figure 2. Conceptual Image of Event Progression Scenario Diagram

Step 4. Categorize mitigation functions.

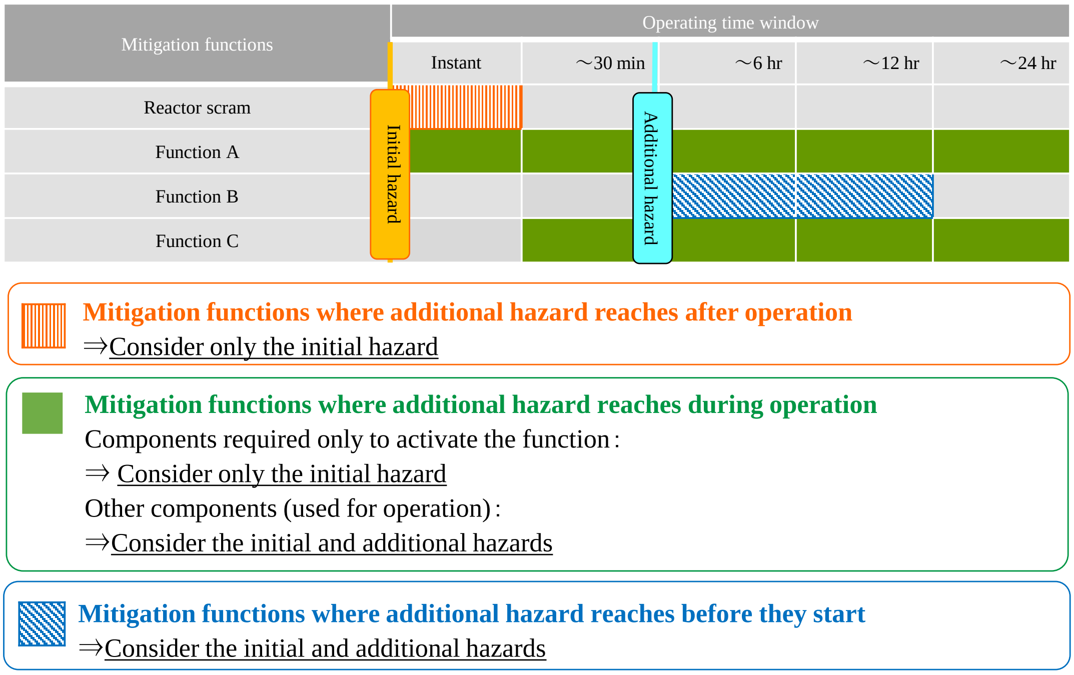
Finally, we identify the mitigation functions and associated events that will be affected by the additional hazard on the event progression scenario diagram created. Figure 3 is an image of a simplified event progression scenario diagram, which visualizes the difference in the extent of impact depending on the arrival time of the additional hazard.

Based on the relationship between the operating time of each mitigation function and the arrival time of additional hazards, the mitigation functions are classified into the following three categories to determine whether or not additional hazard impacts should be considered (see Figure 3).

- Mitigation functions where additional hazard reaches after operation.
- Mitigation functions where additional hazard reaches during operation.
- Mitigation functions where additional hazard reaches before they start.

The mitigation functions where additional hazard reaches after the operation can neglect the damage from the additional hazard. Thus, we need to consider only the damage from the initial hazard. For the mitigation functions where an additional hazard reaches during operation, we need to take the damage from the additional hazard into account with possible exceptions. For components required only to start up the function, we may consider only the initial hazard. Based on the required level of detail for PRA, analysts can select whether to consider the exceptions. The mitigation functions where additional hazard reaches before they start should have influences from the additional hazard. We need to consider the possible damages from both initial and additional hazards.

This procedure allows us to organize the time factors for determining the subject/non-subject of additional hazard impacts according to the hazard impact arrival time scenario for each equipment related to operation in each mitigation function. Note that if several variations of the additional hazard arrival time exist we need to organize the time factors for each possible arrival time variation. Each additional hazard with a different arrival time may have a different source and unique frequency. We need to assess the risk of each possible time variation.



Mitigation functions where additional hazard reaches after operation
⇒Consider only the initial hazard

Mitigation functions where additional hazard reaches during operation
Components required only to activate the function :
⇒ Consider only the initial hazard
Other components (used for operation) :
⇒Consider the initial and additional hazards

Mitigation functions where additional hazard reaches before they start
⇒Consider the initial and additional hazards

Figure 3. Conceptual Image of Classification of Mitigation Functions in Terms of Influence of Additional Hazard

4. EXAMPLE

To show how to use the proposed method, we apply the proposed process to accident sequences of a hypothetical PWR plant created based on public information. We select an earthquake and a tsunami as the initial and additional hazards The time lag between the two hazards is set at two hours. We draw an event progression scenario diagram for accident sequences following a loss of offsite power event.

The timings we estimated are the following three: starting up timing of each mitigation function, completion timing of each mitigation function, and occurrence timing of consequential events, which are induced in the accident sequence after initiating event, such as reactor coolant pump (RCP) seal loss of coolant accident (LOCA). The starting-up timing for each mitigation function is estimated by referring to the timing of a startup signal, the time required to reach the conditions necessary for switching operations, the timing to be ready, and so on. The completion timing is roughly estimated by adding function start time and mission time.

4.1. Gathered Information

Information on the time to be collected for each accident sequence for mitigation system ET was gathered primarily from the following published literature:

- Safety margin assessment (mitigation system ETs for an initiating event induced by seismic impact)
- Internal event PRA (mitigation system ET and success criteria)
- Safety improvement evaluation such as effectiveness evaluation of severe accident management measures (results of thermal hydraulics analysis)
- Overview of Light Water Nuclear Power Stations [5] (standard shutdown curve)

The following is a bulleted list of the evaluation settings that were used in preparing the diagram.

- Startup time of mitigation systems, etc.
  - For systems that are considered to be automatically activated by an initiating event or Consequential LOCA, it is assumed that they are activated at the same time as the event occurs (without taking into account signal time delays, etc.).
  - The minimum time mesh is 0.5 hours (e.g., 25 minutes is approximated as 0.5 hours).
  - The startup time of severe accident management measures is set at the startup time of the system it replaces or the time required to prepare for startup.
  - It is assumed that the air-cooled generators can be started up in a short time (25 minutes) by operation in the main control room, and if that fails, another start-up attempt can be made (former: air-cooled generators (short-term), latter: air-cooled generators (long-term)).
  - Refer to the startup time of the mitigation functions as indicated in the standard shutdown curve (e.g., the startup time of the boric acid addition and the power-operated relief valve (PORV) is 5 hours and 7 hours, respectively).
  - Delays to the startup time of outdoor site response operations for severe accident management measures are not considered.

- Operation end time of mitigation systems, etc.
  - The battery depletion time (assumed to be 5 hours) is assumed for the turbine-driven auxiliary water pump, and the battery is assumed to be recharged by connecting an air-cooled generator.
  - The use of batteries that have been installed as severe accident management measures is not considered.
  - In a scenario where the air-cooled generator can be started simultaneously with the use of the turbine's auxiliary water supply, the batteries are assumed to be float-charged. It is assumed that steam generator (SG) water level monitoring is ensured by the air-cooled generator connection, which is not specified in the scenario.
  - Mode switching time for emergency core cooling system (ECCS)
    - Injection mode: 12 hours
    - Recirculation mode: 72 hours
  - Alternative water injection sequences are not considered because they require boosting by residual heat removal (RHR) pumps.
  - Consider low-pressure injection and low-pressure recirculation by secondary system forced depressurization (switching from a high-pressure injection system and depressurization operation time are not considered).
  - Sequences in which long-term decay heat removal is possible by injecting seawater into the core are not considered.

4.2. Identification of Mitigation Functions Potentially Affected by an Additional Hazard During Accident Progress

For each mitigation function and possible consequential events expected in the accident sequence, the occurrence timing and its completion time are estimated in a simplified manner. A branch is divided according to the success or failure of the function. For both successes and failures, the mitigation functions that are required at the same time or next are connected below, and the timing of the start and the end of the function are estimated in the same way. The same procedure is followed for all accident sequences until reaching the end state of the accident sequence analysis. An event progression scenario diagram was created based on the information collected. Figure 4 shows an excerpt of the event progression scenario diagram for the loss of offsite power.

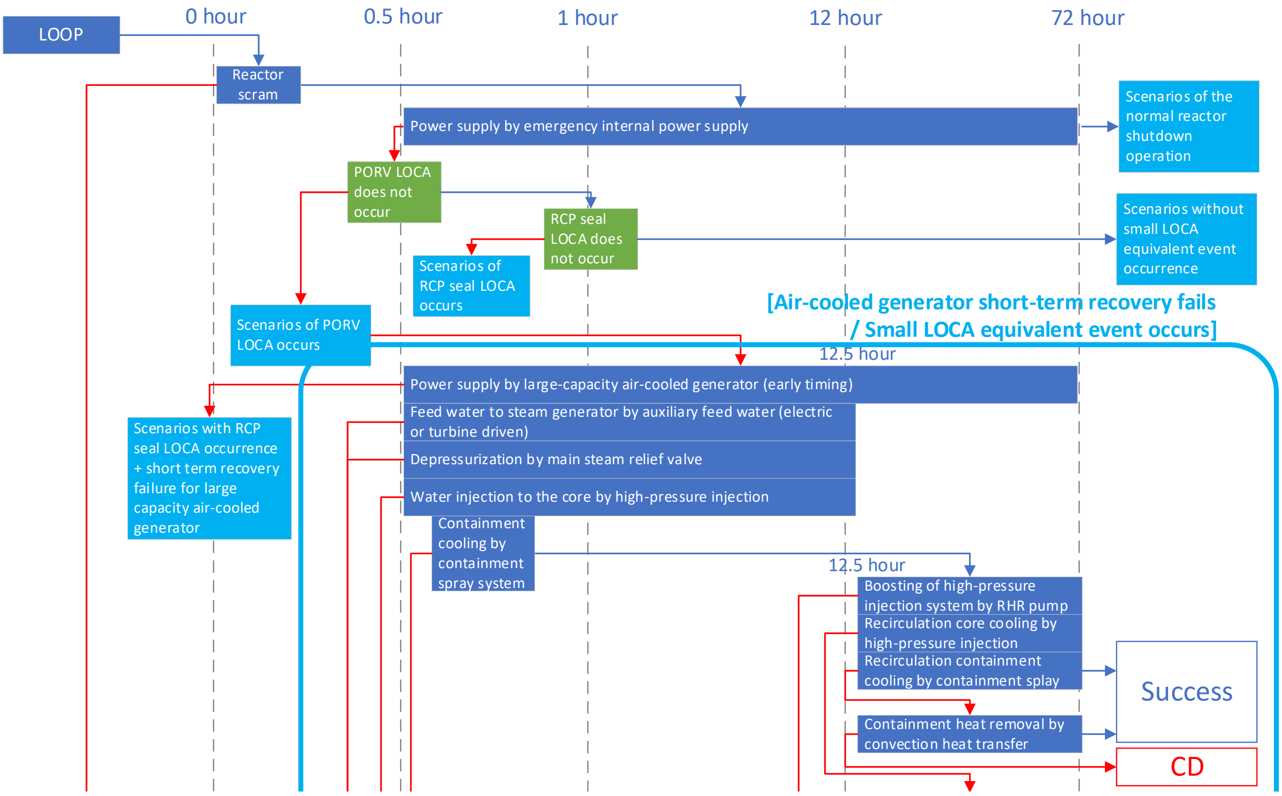


Figure 4. Event Progression Scenario Diagram for Loss of Offsite Power Event (Excerpted)

The arrival timing of an additional hazard, in this case, a tsunami, is overlaid on the operating time of each event and mitigation function in the accident sequence. As shown in Figure 3, we categorize the mitigation functions into three types and determine the modeling policy. Table 1 summarizes the results of the classification of mitigation functions potentially affected by the additional hazard during accident progress.

Table 1. Classification of Mitigation Functions Based on Possibility of Additional Hazard Damage

Classification	Identified Mitigation Functions	Modeling Direction
Mitigation functions that an additional hazard reaches after the operation	• Reactor scram • RCP seal LOCA / PORV LOCA • Containment cooling by containment spray system	The impact of the tsunami is negligible.
Mitigation functions that an additional hazard reaches during operation	• Power supply by emergency internal power supply • Power supply by large-capacity air-cooled generator (early timing) • Feed water to the steam generator by auxiliary feed water (electric or turbine driven) • Depressurization by main steam relief valve • Water injection to the core by high-pressure injection	The impact of the tsunami is NOT negligible on the components required to activate the system.
Mitigation functions that an additional hazard reaches before they start	• Activating of a high-pressure injection system by residual heat removal pump • Recirculation core cooling by high-pressure injection • Recirculation containment cooling by containment splay • Containment heat removal by convection heat transfer • Depressurization by main steam relief valve (forced open) • Recirculation core cooling by low-pressure injection	The impact of the tsunami is NOT negligible.

4.3. Insights Obtained through Demonstration

The notes obtained through the demonstration based on publicly available information are summarized as follows:

- In many scenarios, tsunamis are expected to arrive during operation in the injection mode as the arrival time difference of the hazard impact is about 2 hours or less. Thus, few mitigation functions can avoid the tsunami impact.
- Although the minimum unit of time mesh in this example is 0.5 hours, the time mesh for the event progression scenario for model consistency should be set depending on the fineness of the hazard impact arrival time difference and the uncertainty of the hazard. Note that too fine a time unit would increase the variation of scenarios, which in turn would increase the cost of the PRA analysis.
- When developing a containment event tree for a Level 2 PRA, it may be necessary to consider the impact of mitigation functions that work until the additional hazard makes them fail before their mission times.

5. CONCLUSION

This study has proposed a method to consider the effects of additional hazards on the accident sequence model following initiating events induced by the first hazard. The proposed method is based on “event progression scenario diagrams,” which organize information on accident sequences in chronological order and show how to identify SSCs that are affected by additional hazards. We presented an example of the application of the proposed method using a hypothetical model based on publicly available information. Although the method was proposed for application to a combined hazard PRA, its applicability to similar scenarios in which additional hazards are acting during accident progression is also considered feasible. For example, it could be used in the context of a multi-unit PRA to reflect the effects of an explosion event occurring in an adjacent unit.

References

[1] Committee on Tsunami Resistant Engineering for Nuclear Safety, Japan Association for Earthquake Engineering (JAEE), “Tsunami resistant engineering for nuclear safety – toward an integrated framework for earthquake-tsunami protection. –”, JAEE report, 2015.

[2] Berg H.-P. and Roewekamp M., “Natural Hazards: Systematic Assessment of Their Contribution to Risk and Their Consequences” In Kostogryzov, A. (Ed.). Probabilistic Modeling in System Engineering (pp. 125-143). InTechOpen. 2018.

[3] Miura, H., Soga, S., and Higo, E., “Development of Methods for Internal Event Level 1 Multi-Unit Probabilistic Risk Assessment” CRIEPI Report NR22003, 2023. The Internet address is https://criepi.denken.or.jp/hokokusho/pb/reportDownload?reportNoUkCode=NR22003&tenpuTypeCode=40&seqNo=2&reportId=9934

[4] Miura, H., Soga, S., and Higo, E., "An evaluation method for a seismic-induced multi-unit initiating event extending an initiating event classification tree for a nuclear power station." Mechanical Engineering Journal 11.2, 2024.

[5] Enomoto T. (Ed.), “Overview of Light Water Nuclear Power Stations”, Nuclear Safety Research Association, Japan, 2010.