A Framework for Seismic Design of Items in Safety-Critical Facilities for Implementing a Risk-Informed Defense-in-Depth-Based Concept

Tatsuya Itoi*, Yuki Iita and Naoto Sekimura

School of Engineering, The University of Tokyo, Tokyo, Japan

Recently, especially after the 2011 off the Pacific coast of Tohoku earthquake and the Fukushima Daiichi nuclear power plant accident, the need for treating residual risks and cliff-edge effects in safety-critical facilities has been widely recognized as an extremely important issue. In this article, the sophistication of seismic designs in safety-critical facilities is discussed from the viewpoint of mitigating the consequences of accidents, such as the avoidance of cliff-edge effects. For this purpose, the implementation of a risk-informed defense-in-depth-based framework is proposed in this study. A basic framework that utilizes diversity in the dynamic characteristics of items and also provides additional seismic margin to items important for safety when needed is proposed to prevent common cause failure and to avoid cliff-edge effects as far as practicable. The proposed method is demonstrated to be effective using an example calculation.

Keywords: seismic design, risk, safety-critical facility, defense in depth, cliff-edge effects

INTRODUCTION

Natural hazards, including earthquakes, are considered to be one of several possible causes of major accidents in safety-critical facilities such as nuclear power plants. Conventionally, it had been required, when designing safety-critical facilities against earthquakes, that design ground motion must be determined so that risks, e.g., to public health, associated with ground motion hazards are negligible compared with those associated with accidents of internal origins (International Atomic Energy Agency, 1988). It has been occasionally misunderstood that seismic safety of safety-critical facilities can be achieved if design ground motion is set large enough so that seismic risks can be sufficiently reduced. Recently, however, especially after the 2011 off the Pacific coast of Tohoku earthquake and the Fukushima Daiichi nuclear power plant accident, the need for serious consideration and treatment of residual risks has been widely recognized as an extremely important issue. Although the accident was caused due to tsunami, it was also recognized that there exists a room for discussion also for a framework of earthquake engineering.

A framework of performance-based seismic design (Structural Engineers Association of California, 1995) is considered to be one of several reasonable approaches in the practice of seismic design of engineering facilities. Within this framework, as shown in **Figure 1**, the levels of design ground motion are specified so that several performance objectives are met, and these levels are specified based on the potential severity of consequences when facilities suffer from damage.

FIGURE 1 | Typical framework for performance-based seismic design (Structural Engineers Association of California, 1995).
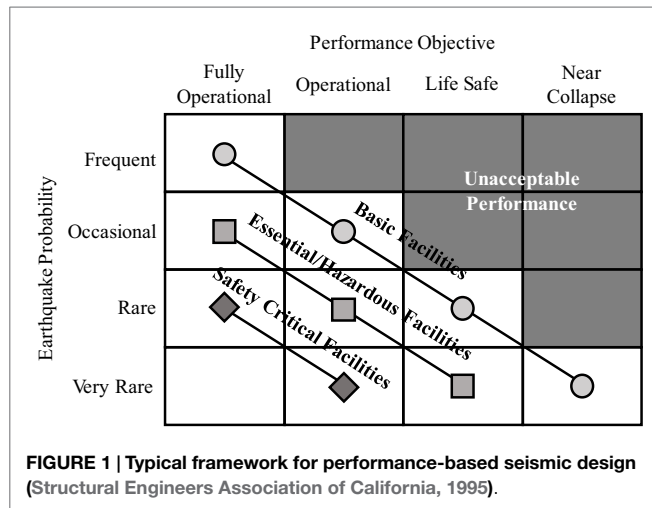
For safety-critical facilities, it is required to be operational even in the case of very rare earthquakes, i.e., severe earthquakes, and a near collapse state is not acceptable for any level of earthquake. On the other hand, a near collapse state is acceptable for basic facilities in the event of very rare earthquakes. What should be emphasized here is that this framework does not imply that safety-critical facilities do not require a mitigation strategy in dealing with the consequences of failure to the extent where these facilities are severely damaged to the point of collapse. Such a strategy, nonetheless, is considered to be more important for safety-critical facilities than for basic facilities.

In the field of nuclear safety, the "defense-in-depth" concept is considered to be important when dealing with residual risks, i.e., remaining risks after safety measures are introduced, and it is the primary means to prevent and mitigate the consequences of accidents (International Atomic Energy Agency, 1996, 2006). For safety-critical facilities, the defense-in-depth concept is implemented through a combination of consecutive and independent levels of protection (International Atomic Energy Agency, 1996, 2006). The central feature of the defense in depth is the idea of multiple levels of protection of public and workers (International Atomic Energy Agency, 1996). Under seismic excitations, however, it is impossible and unrealistic to assume that each level of protection for defense in depth is completely independent of each other. This is because items corresponding to each level of defense are simultaneously excited by earthquake ground motion in space and time, and this could lead to simultaneous malfunction and/or damage that results in a common cause failure. If items that are important in preventing accidents and mitigating the consequences of accidents simultaneously malfunction and/or suffer from damage, accidents with serious consequences could occur. These kinds of effects in the event of accidents are also known as cliff-edge effects (International Atomic Energy Agency, 2003, 2016a,b). The term "cliff-edge effects" implies a sudden large variation in condition of the facilities in response to a small variation in an input. It is triggered by simultaneous malfunction of these items.

There appears to be, however, no widely accepted approach in implementing the defense-in-depth concept over a wide range of seismic excitations, because the concept of the defense in depth was originally developed for accidents of internal origins. Therefore, this article proposes a basic theoretical framework with respect to seismic design of items important to safety based on a risk-informed concept (United States Nuclear Regulatory Commission, 2012), so that the defense-in-depth concept can be appropriately implemented for the seismic safety of safety-critical facilities.

As mentioned earlier, multiple items in a facility are excited and some of them are damaged by earthquake ground motions simultaneously. Moreover, spatially distributed multiple facilities suffer from damage simultaneously. These characteristics should be taken into consideration when conducting seismic risk assessment (Bazzurro and Cornell, 2002; Wang et al., 2009). Ground motion modeling, which can be applied to such seismic probabilistic risk assessment, has also been developed (Wang and Takada, 2005; Baker and Jayaram, 2008). In this study, a basic implementation method to deal with such characteristics of ground motions, called "risk-informed defense-in-depth-based framework" (Miyano et al., 2015), is developed by using this risk-based framework. The proposed method combines the concepts of diversity and seismic margin for the framework to give a basic insight on how multiple items closely located to each other can be designed to cope with earthquakes by combining multiple barriers.

PROPOSED FRAMEWORK OF SEISMIC DESIGN OF ITEMS IMPORTANT TO SAFETY

Background and Assumption

Items important to safety can be simply categorized into items that are important in preventing accidents and items that are important in mitigating the consequences of accidents. Items important to mitigating the consequences of accidents are required to function only after the occurrence of an accident, which essentially means that items important in preventing accident, in the first place, are damaged and/or have malfunctioned. Conventional seismic design procedures, however, do not usually distinguish between the roles of these two items.

The strategy for items important for safety is considered to be developed by combining diversity, physical separation, and functional independence (International Atomic Energy Agency, 2016a). Implementation of physical separation and functional independence is considered to be straightforward, while implementation of diversity to seismic excitation needs to be discussed further. Therefore, implementation of diversity to seismic excitation is discussed in this article. Diversity is provided by different mechanisms to function. In the seismic design of facilities, diversity is considered to be provided through differences in location of items (such as a plan layout or elevation) and by different dynamic characteristics between items (such as structural type, natural period, and damping characteristics). Providing an additional seismic margin, such as differentiation in classes of required seismic margins to each item based on its role, is another means in avoiding cliff-edge effects (International Atomic Energy Agency, 2016a). Typically, conservative parameters are introduced in the

analysis of seismic design to deal with uncertainty, which are based on engineering judgment, the results of structural analysis, etc. These conservative parameters result in conservative designs. Quantification of such conservativeness is important to discuss the performance of facility to ground motions greater than the design ground motion (Budnitz et al., 1985; Haselton et al., 2011). In this study, an appropriate combination of seismic margin and diversity is discussed to implement the defense-in-depth concept to seismic design for safety-critical facility based on the risk-informed approach. A method to assign required additional seismic margins to each item is proposed depending on the characteristics of diversity introduced. As mentioned earlier, diversity is important to implement the defense-in-depth concept under seismic excitations. It is, however, not always possible to introduce it, because of the limitation due to the characteristics of item. Additional seismic margin is considered to be effective as a means of supplementing for such cases. Here, additional seismic margin means that seismic margin is required in addition to the seismic margin that is already introduced in the conventional seismic design.

A Method to Identify the Most Probable Source Characteristics and Associated Ground Motion Parameters That May Cause Accidents at Safety-Critical Facilities

Probabilistic Seismic Hazard Analysis and Ground Motion Prediction Equation

Probabilistic seismic hazard analysis is used to determine design ground motion and to analyze seismic risk of facilities. An example of the annual exceedance probability of design ground motion required for safety-critical facilities is usually $\sim 10^{-4}$ or smaller (Nuclear Regulatory Commission, 1997, 2007). Statistical equations, called ground motion prediction equations, are conventionally used to predict ground motions. In all, 5% damped acceleration response spectra are conveniently used to characterize a variety of frequency contents in different ground motions. A ground motion prediction equation for 5% damped spectral acceleration that is used in this study was initially developed for crustal earthquakes in Japan (Itoi et al., 2015). The functional form of the equation is as follows (Itoi et al., 2015):

$$
\begin{aligned}
\log_{10} S_{a\mathrm{GM}}(T) = {} & a(T) + b(T)M_W - c(T)X \\
& - \log_{10}\left(X + d(T) \cdot 10^{0.5 M_W}\right) \\
& - e(T)\left(\log_{10} V_{S30}\right)^2 + f(T)\log_{10} V_{S30} \\
& + g(T)\log_{10}\left(\max\left(\min\left(Z_{1500}, h(T)\right), k(T)\right)\right) \\
& + \sigma_{\mathrm{INTER}}(T)E_{\mathrm{INTER}}(T) + \sigma_{\mathrm{INTRA}}(T)E_{\mathrm{INTRA}}(T)
\end{aligned}
\tag{1}
$$

where $S_a(T)$ is the 5% damped spectral acceleration at period T. M_W, X (km), V_{S30} (m/s), and Z_{1500} (m) are the moment magnitude, the shortest distance from fault to site, the 30 m average shear wave velocity, and the depth to shear wave velocity, which is equal to 1,500 m/s, respectively. $E_{\mathrm{INTER}}(T)$

and $E_{\mathrm{INTRA}}(T)$ are standard normal variables for inter-event and intra-event residuals, respectively, while $\sigma_{\mathrm{INTER}}(T)$ and $\sigma_{\mathrm{INTRA}}(T)$ are their corresponding standard deviations. $a(T)$ to $k(T)$ are the coefficients obtained by the least-square regression. The coefficients $a(T)$ to $k(T)$, $\sigma_{\mathrm{INTER}}(T)$, and $\sigma_{\mathrm{INTRA}}(T)$ obtained based on the least-square regression are summarized in **Table 1**. Period-to-period correlations for inter-event residuals $\rho_{\mathrm{INTER}}(T_A, T_B)$ and intra-event residuals $\rho_{\mathrm{INTRA}}(T_A, T_B)$ are summarized in **Table 2**. Correlation of $E_{\mathrm{INTER}}(T)$ and $E_{\mathrm{INTRA}}(T)$ between different periods T is important when the possibility of simultaneous damage of multiple items, i.e., a common cause failure, is discussed. The applicable range of the equation is $5.1 \leq M_W \leq 6.9$, $X \leq 100$ km, 110 m/s $\leq V_{S30} \leq 700$ m/s, and $Z_{1500} \leq 3{,}000$ m (Itoi et al., 2015).

A Method to Identify the Most Probable Source Characteristics

In this section, a framework is proposed to identify the most probable source characteristics and ground motion parameters that may result in accidents. The most probable source characteristics and ground motion parameters are defined here as the design point that can be obtained by the first-order reliability method (FORM) (Rackwitz and Fiessler, 1978). The design point is defined as the point with the highest probability density in the domain of accident. The FORM (Rackwitz and Fiessler, 1978), probabilistic seismic hazard deaggregation (McGuire, 1995; Takada et al., 2003), and the conditional mean spectrum (Baker, 2011) are used in the proposed framework.

A system that is considered for a simplified case is assumed to contain two items (items A and B) that are located at the same place. It is assumed that an accidental condition occurs if item A fails. Item B is then used to mitigate the consequences of the resulting accident. A fault tree representation of system failure defined by an occurrence of an accident with serious consequences is shown in **Figure 2** using the priority-AND gate. Item A is assumed to be a single-degree-of-freedom system that has a natural period T_A. The limit state function for failure of item A, G_A, is defined as follows:

$$
G_A = R_A(T_A) - S_A(T_A)
\tag{2}
$$

where $R_A(T_A)$ is the capacity of item A as a function of the 5% damped spectral acceleration at $T = T_A$ and is assumed to have a log-normal distribution. $S_A(T_A)$ is the maximum seismic action on item A, i.e., 5% damped spectral acceleration at $T = T_A$. The probability distribution of $S_A(T_A)$ for a certain period of time, which is 1 year in this case, is obtained using the probabilistic seismic hazard analysis. Item A fails if G_A is negative, while item A survives if G_A is positive. The most probable level of spectral acceleration $s_A{}^*$ for $S_A(T_A)$ is obtained using FORM.

Then, the most probable earthquake source parameters and ground motion parameters that may result in accidents are identified. Similar to Eq. 2, a limit state function G_{HA} is defined as follows:

$$
G_{\mathrm{HA}} = \log_{10} s_A{}^* - \log_{10} S_{\mathrm{CA}}(T_A)
\tag{3}
$$

TABLE 1 | The coefficients for the ground motion prediction equation (Itoi et al., 2015).

T(s)	a	b	c (×10⁻³)	d (×10⁻³)	e	f	g	h	k	σ_{INTER}	σ_{INTRA}
0.02	−8.202	0.5462	2.909	3.955	−1.508	7.226	–	–	–	0.2068	0.2446
0.04	−7.576	0.5154	3.218	4.631	−1.377	6.762	–	–	–	0.2197	0.2474
0.06	−7.076	0.4936	2.823	4.549	−1.267	6.376	–	–	–	0.2253	0.2639
0.11	−13.26	0.5285	2.428	3.851	−2.314	11.45	–	–	–	0.2195	0.2715
0.19	−14.40	0.5852	2.843	2.651	−2.644	12.60	–	–	–	0.2038	0.2795
0.32	−8.716	0.6585	3.213	1.982	−1.759	7.867	–	–	–	0.1948	0.2777
0.56	0.2375	0.7416	3.148	1.144	−0.263	0.116	0.1279	988.4	12.19	0.1926	0.2788
0.97	4.066	0.8234	3.728	1.238	0.512	−3.721	0.1909	968.8	7.664	0.1860	0.2718
1.7	0.6731	0.9358	4.644	2.493	0.193	−1.966	0.2135	–	9.785	0.1625	0.2501
2.9	0.4002	0.9731	3.809	3.421	0.380	−2.731	0.3573	–	100.9	0.1265	0.2257
5.0	−1.629	1.063	2.204	4.502	0.271	−2.028	0.3410	–	131.5	0.1047	0.2080

TABLE 2 | Period-to-period correlation for inter-event and intra-event residuals (Itoi et al., 2015).

T(s)	0.02	0.04	0.06	0.11	0.19	0.32	0.56	0.97	1.7	2.9	5.0
(A) Inter-event residuals $\rho_{INTER}(T_1, T_2)$											
0.02	1	0.9928	0.9811	0.9877	0.9841	0.9284	0.8333	0.7689	0.7007	0.2367	0.0716
0.04		1	0.9942	0.9867	0.9655	0.8868	0.7917	0.7345	0.6742	0.2200	0.0614
0.06			1	0.9867	0.9509	0.8569	0.7563	0.6971	0.6368	0.2222	0.0632
0.11				1	0.9740	0.8930	0.7830	0.7141	0.6503	0.2380	0.0706
0.19					1	0.9490	0.8436	0.7681	0.6887	0.2653	0.1013
0.32						1	0.9326	0.8540	0.7520	0.2703	0.1276
0.56							1	0.9596	0.8677	0.3285	0.1944
0.97				Sym.				1	0.9303	0.4126	0.3179
1.7									1	0.5987	0.4917
2.9										1	0.8011
5.0											1
(B) Intra-event residuals $\rho_{INTRA}(T_1, T_2)$											
0.02	1	0.9568	0.9022	0.8976	0.8048	0.6247	0.4673	0.3294	0.2541	0.2428	0.2865
0.04		1	0.9501	0.8570	0.7061	0.5133	0.3592	0.2294	0.1583	0.1555	0.1911
0.06			1	0.8362	0.6153	0.4158	0.2737	0.1524	0.0903	0.0990	0.1337
0.11				1	0.7007	0.4519	0.3054	0.1991	0.1458	0.1551	0.2050
0.19					1	0.7257	0.5306	0.3996	0.3188	0.2954	0.3372
0.32						1	0.7485	0.5702	0.4521	0.3779	0.3966
0.56							1	0.7764	0.6156	0.5218	0.4969
0.97				Sym.				1	0.7926	0.6457	0.5793
1.7									1	0.7920	0.6628
2.9										1	0.7956
5.0											1

where $S_{CA}(T_A)$ is the ground motion given the earthquake occurrence. Based on Eq. 1, $S_{CA}(T_A)$ is described as follows:

$$\log_{10} S_{CA}(T_A) = a(T_A) + b(T_A) M_W - c(T_A) X$$
$$- \log_{10}\left(X + d(T_A) \cdot 10^{0.5 M_W}\right)$$
$$- e(T_A)\left(\log_{10} v_{S30S}\right)^2 + f(T_A) \log_{10} v_{S30S}$$
$$+ g(T_A) \log_{10}\left(\max\left(\min\left(z_{1500S}, h(T_A)\right), k(T_A)\right)\right)$$
$$+ \sigma_{INTER}(T_A) E_{INTER}(T_A)$$
$$+ \sigma_{INTRA}(T_A) E_{INTRA}(T_A)$$

$$(4)$$

where M_W, X, $E_{INTER}(T_A)$, and $E_{INTRA}(T_A)$ are random variables representing the moment magnitude, the shortest distance from fault to site, the standard normal variable for inter-event residual, and the standard normal variable for intra-event residual, respectively. v_{S30S} and z_{1500S} are V_{S30} and Z_{1500} at the location of the system, respectively.
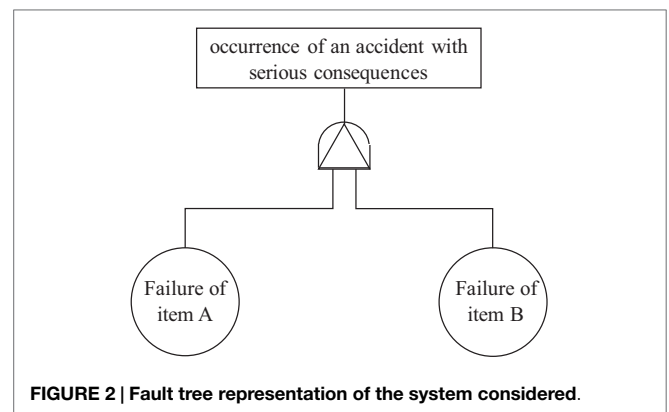

FIGURE 2 | Fault tree representation of the system considered.

The most probable values for M_W, X, $E_{INTER}(T_A)$ and $E_{INTRA}(T_A)$, M_W^*, x^*, $\varepsilon_{INTER}^*(T_A)$, and $\varepsilon_{INTRA}^*(T_A)$ are obtained given that $S_A(T_A) = s_A^*$ using FORM. The

methodology used is almost identical to that proposed by Takada et al. (2003) and similar to that proposed by McGuire (1995).

Item B is also assumed to be a single-degree-of-freedom system with a natural period T_B, which can be different from T_A. The most probable earthquake source characteristics under which item B is required to function is an earthquake of magnitude $M_W{}^*$, whose shortest distance from fault to site is x^*. The most probable spectral acceleration at period T_A is $s_A{}^*$, which is obtained from Eq. 3 using the abovementioned procedure. The most probable spectral acceleration at period T_B, $\bar{s}_B{}^* (T_B|T_A)$, given this condition, is calculated as follows:

$$
\begin{aligned}
\log_{10}\bar{s}_B{}^* (T_B|T_A) = {} & a(T_B) + b(T_B) M_W{}^* - c(T_B) x^* \\
& - \log_{10}\left(x^* + d(T_B)\cdot 10^{0.5 M_W{}^*}\right) \\
& - e(T_B)\left(\log_{10} V_{S30S}\right)^2 + f(T_B)\log_{10} V_{S30S} \\
& + g(T_B)\log_{10}\left(\max\left(\min\left(Z_{1500S}, h(T_B)\right), k(T_B)\right)\right) \\
& + \sigma_{\text{INTER}}(T_B)\bar{\varepsilon}_{\text{INTER}}{}^* (T_B|T_A) \\
& + \sigma_{\text{INTRA}}(T_B)\bar{\varepsilon}_{\text{INTRA}}{}^* (T_B|T_A)
\end{aligned}
\tag{5}
$$

where $\bar{\varepsilon}_{\text{INTER}}{}^* (T_B|T_A)$ and $\bar{\varepsilon}_{\text{INTRA}}{}^* (T_B|T_A)$ are the conditional means of the bivariate normal distribution given $\varepsilon_{\text{INTER}}{}^* (T_A)$ and $\varepsilon_{\text{INTRA}}{}^* (T_A)$, respectively, as follows:

$$
\bar{\varepsilon}_{\text{INTER}}{}^* (T_B|T_A) = \frac{\rho_{\text{INTER}}(T_A, T_B)\,\varepsilon_{\text{INTER}}{}^* (T_A)}{\sqrt{1 - \rho_{\text{INTER}}(T_A, T_B)^2}}
\tag{6}
$$

$$
\bar{\varepsilon}_{\text{INTRA}}{}^* (T_B|T_A) = \frac{\rho_{\text{INTRA}}(T_A, T_B)\,\varepsilon_{\text{INTRA}}{}^* (T_A)}{\sqrt{1 - \rho_{\text{INTRA}}(T_A, T_B)^2}}
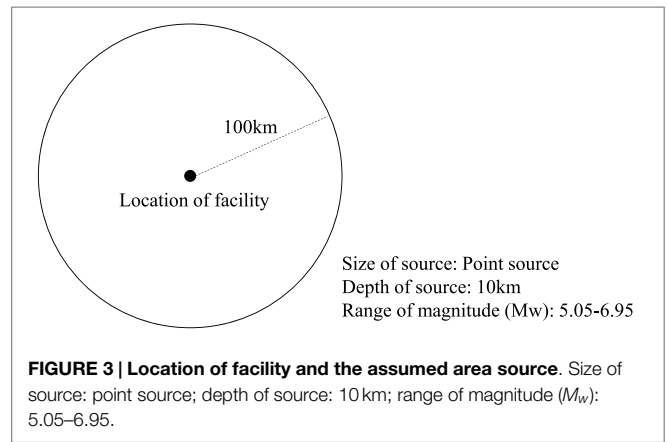\tag{7}
$$

This concept is identical to that of the conditional mean spectrum proposed by Baker (2011). As can be understood from Eqs 6 and 7, $\bar{\varepsilon}_{\text{INTER}}{}^* (T_B|T_A)$ and $\bar{\varepsilon}_{\text{INTRA}}{}^* (T_B|T_A)$ respectively, approach asymptotically to 0 as the difference between T_A and T_B increases. This is because $\rho_{\text{INTER}}(T_A, T_B)$ and $\rho_{\text{INTRA}}(T_A, T_B)$ approach 0 as the difference between T_A and T_B increases as shown in **Table 2**.

Proposed Framework to Provide Additional Seismic Margins to Items Important in Mitigating the Consequences of Accidents

Item B should be designed based on a different concept from that of item A. It is because a role of item B is different from that of item A. Therefore, it has been proposed in this study that the seismic margin $m_B(T_B|T_A)$, which is additionally required for item B, is a function of the obtained spectral acceleration $\bar{s}_B{}^* (T_B|T_A)$ and is given as follows:

$$
m_B(T_B|T_A) = \max\left(1, \frac{\bar{s}_B{}^* (T_B|T_A)}{s_{\text{BD}}(T_B)}\right)
\tag{8}
$$

where $S_{\text{BD}}(T_B)$ is the spectral acceleration at period T_B for the original seismic design obtained using the same concept as that

FIGURE 3 | Location of facility and the assumed area source. Size of source: point source; depth of source: 10 km; range of magnitude (M_w): 5.05–6.95.

for item A. From Eq. 5, it can be found that the additional seismic margin $m_B(T_B|T_A)$ is almost unity if the difference between T_A and T_B is large enough. This is justified because diversity with respect to dynamic characteristics, such as the natural period, is expected to work effectively. (This will be discussed in the next chapter.). On the other hand, a larger additional margin $m_B(T_B|T_A)$ is required if T_A and T_B are close to each other, i.e., if the diversity in the characteristics of items is not introduced in the seismic design. The proposed method combines the information on regional seismicity, the characteristics of ground motions, and the vulnerability of the facility to determine the additional seismic margin required for items that are important in mitigating the consequences of accidents.
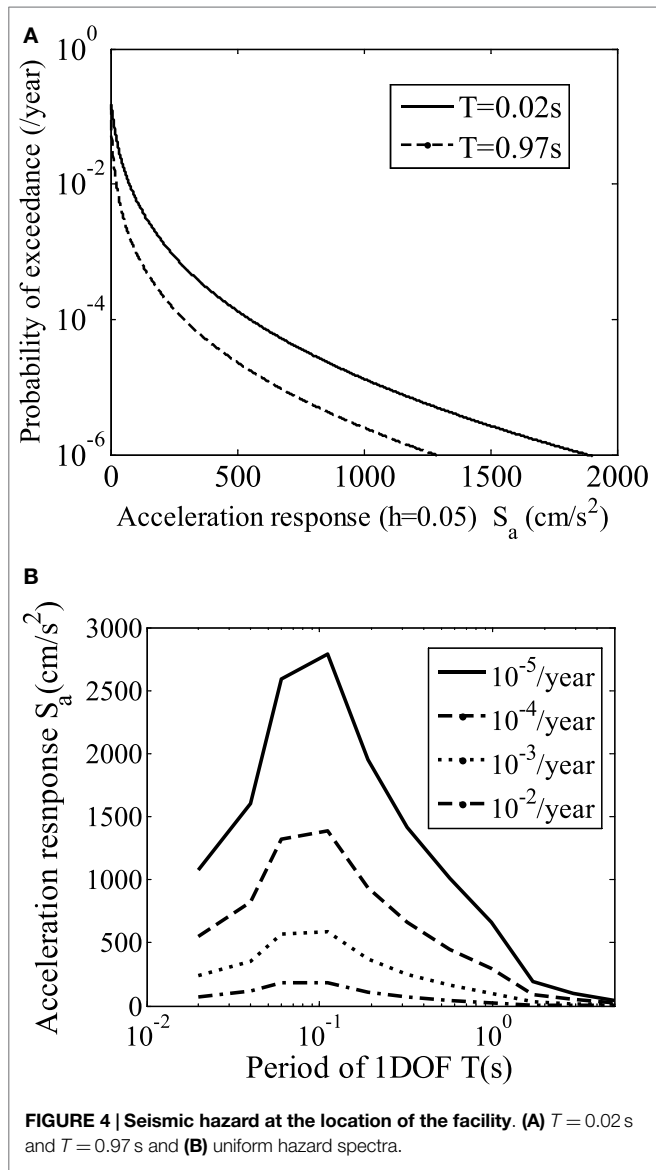
SEISMIC MARGIN REQUIRED FOR ITEMS THAT ARE IMPORTANT IN MITIGATING THE CONSEQUENCES OF ACCIDENTS FOR AREA SOURCES

Simulation Conditions

An area source as shown in **Figure 3** is used as an example. Point sources are uniformly distributed within a radius of 100 km, whereby their focal depth is 10 km. The facility is assumed to be located on the ground surface above the center of the area source. The probability distribution of the earthquake magnitude is assumed to be in agreement with the Gutenberg–Richter law. The cumulative distribution function for the magnitude $F_M(m)$ is as follows:

$$
F_M(m) = \frac{\exp(-b\cdot \ln10\cdot m) - \exp(-b\cdot \ln10\cdot m_{\min})}{\exp(-b\cdot \ln10\cdot m_{\max}) - \exp(-b\cdot \ln10\cdot m_{\min})}
\tag{9}
$$

where $m_{\max}$ (6.95) and $m_{\min}$ (5.05) are the maximum and minimum magnitudes, respectively. b is assumed to be 0.9. These values are typical for those used for earthquakes without specified source faults in Japan. v_{S30S} and z_{1500S} of Eq. 5 are assumed to be 700 m/s and 100 m, respectively. v_{S30S} and z_{1500S} are the 30 m average shear wave velocity and the depth to shear wave velocity, which is equal to 1,500 m/s at the site, respectively. Seismic hazard curves and uniform hazard response spectra calculated at the facility are shown in **Figure 4**. The design ground motion for a
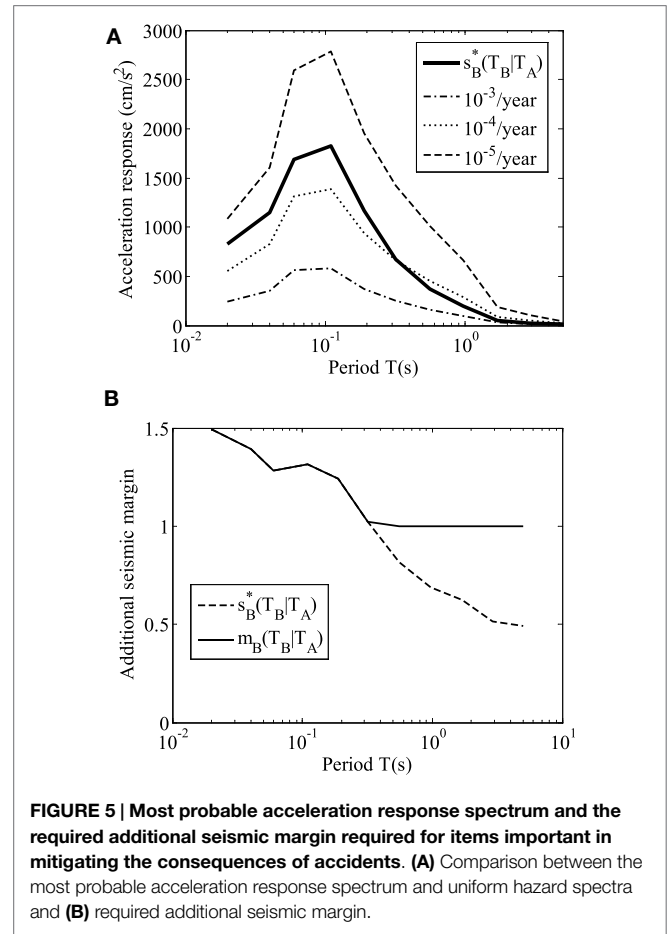
FIGURE 4 | Seismic hazard at the location of the facility. (A) $T = 0.02$ s and $T = 0.97$ s and (B) uniform hazard spectra.

TABLE 3 | Three alternative options for item B.

Case 0 (item B_0)	Natural period of item B is 0.02 s, which is identical to that of item A Item B is designed for design ground motion corresponding to the exceedance probability of 10^{-4}/year
Case S (item B_S)	Natural period of item B is 0.02 s, which is identical to that of item A Seismic margin is provided based on the proposed method (Eq. 8)
Case T (item B_T)	Natural period of item B is 0.97 s Seismic margin is provided based on the proposed method (Eq. 8)

FIGURE 5 | Most probable acceleration response spectrum and the required additional seismic margin required for items important in mitigating the consequences of accidents. (A) Comparison between the most probable acceleration response spectrum and uniform hazard spectra and (B) required additional seismic margin.

system is assumed to correspond to the exceedance probability of 10^{-4}/year.

The facility is modeled as a system that contains two items, items A and B, as is the case in Section "A Method to Identify the Most Probable Source Characteristics." The natural period of item A, T_A, is assumed to be 0.02 s. As for item B, three alternative options (items B_0, B_S, and B_T) are assumed as listed in **Table 3**. It is assumed as an example that the logarithmic standard deviation of the capacity of each item is 0.3, while the conditional probability of failure at the level of design ground motion is 0.01. The most probable spectral acceleration and additional seismic margin required for items that are important in mitigating the consequences of accidents (items B_S and B_T) are obtained based on the proposed method as shown in **Figure 5**. Seismic fragility curves that show the cumulative distribution function of the capacity as a function of 5% spectral acceleration at the natural period, assumed for items B_0, B_S, and B_T, are shown in **Figures 6A,B**.

The most probable source characteristics and the most probable ground motion parameters that may cause accidents are shown in **Table 4**. An additional seismic margin of 1.49 for item B_S, as compared to item B_0, is obtained using Eq. 8 for this example, whereas an additional seismic margin is not required for item B_T. If two items have the similar mechanism to resist seismic forces, it is reasonable to assume that the capacities between them are correlated. Therefore, for cases 0 and S, the correlation coefficient ρ between the capacities of A and B is assumed to be 0, 0.3, and 0.6, i.e., for items B_0 and B_S, where $\rho = 0$ for reference. Independence between items A and B_T is assumed for case T.

Monte Carlo simulations are conducted where the number of samples for the simulation is 10^8. Samples of hypocenter and magnitude of earthquakes, 5% damped acceleration response spectra, and capacity of items are generated to calculate the fragility curve
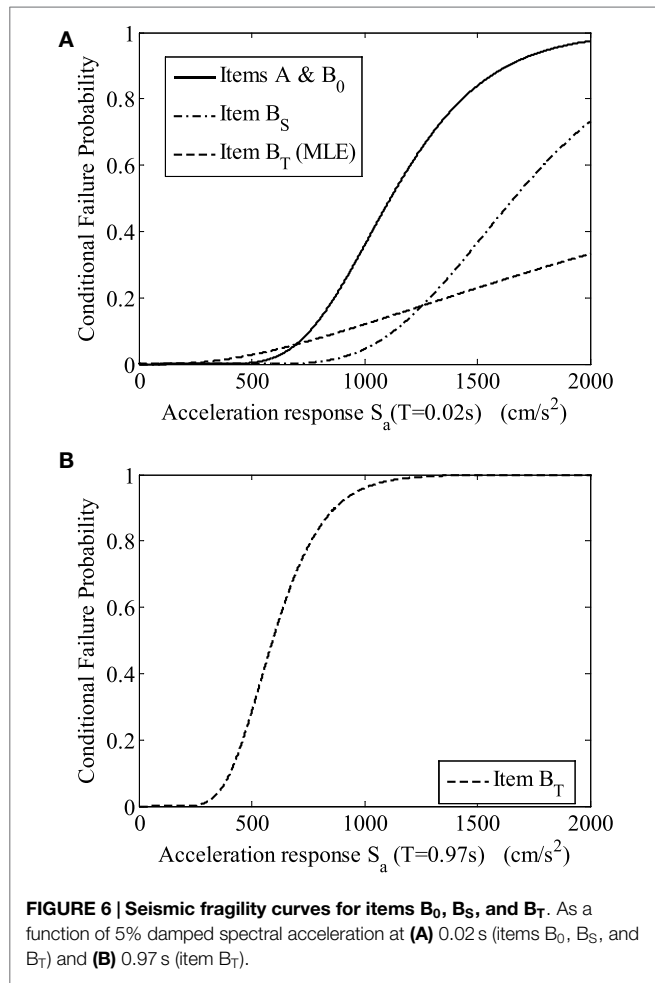
FIGURE 6 | Seismic fragility curves for items B₀, Bₛ, and Bᴛ. As a function of 5% damped spectral acceleration at **(A)** 0.02 s (items B₀, Bₛ, and Bᴛ) and **(B)** 0.97 s (item Bᴛ).

TABLE 4 | Most probable source characteristics and the most probable ground motion parameters that may cause accidents.

$s_A{}^*$ (cm/s²)	$M_W{}^*$	x^* (km)	$\varepsilon_{INTER}{}^*(T_A)$	$\varepsilon_{INTRA}{}^*(T_A)$
824	6.47	15	0.283	0.396

for failure of the system, i.e., simultaneous malfunction of both items.

Results and Discussions

Seismic fragility curves for item B_T as a function of 5% damped spectral acceleration at 0.02 s are estimated based on the simulated samples using the maximum likelihood estimation (Shinozuka et al., 2000), as shown in **Figure 6A**. The logarithmic standard deviation obtained is 0.93, which includes the effects of uncertainties in the shape of acceleration response spectra and the capacity of the item.

Seismic fragility curves of the system representing the cumulative distribution as a function of 5% damped spectral acceleration at 0.02 s, for the occurrence of a simultaneous malfunction of two items, are also obtained using the maximum likelihood estimation (Shinozuka et al., 2000). These are shown in **Figure 7**. As for case 0, i.e., item B_0, the median capacity of the system is 1.2 times
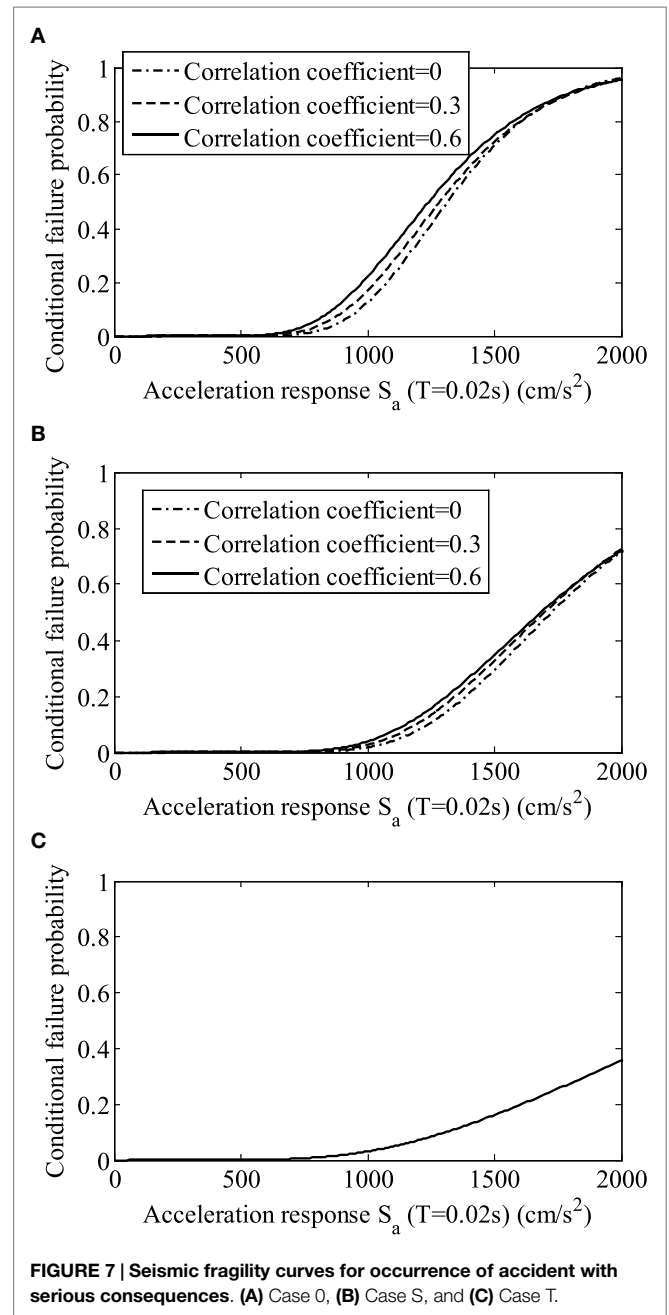

FIGURE 7 | Seismic fragility curves for occurrence of accident with serious consequences. (A) Case 0, **(B)** Case S, and **(C)** Case T.

larger than that of item A when $\rho = 0$, while it is 1.1 times larger when $\rho = 0.6$. The median capacity decreases as the correlation coefficient ρ increases because of simultaneous damage of two items. As for case S where an additional seismic margin is provided to item B, the median capacity of the system is 1.5 times larger than that of item A when $\rho = 0$, 0.3, and 0.6. The difference between ρ can be observed for ground motion <2,000 cm/s². As for case T, the case that the natural period of item B is elongated, the median capacity of the system is 2.1 times larger than that of item A, while the logarithmic standard deviation is 0.47, and this is larger than those in case 0 (0.24–0.28) and case S (0.26–0.30). Case T is more effective for larger ground motion levels as compared to cases 0 and S.

TABLE 5 | Calculated failure probabilities for the system.

Case	Failure probability of the system (per year)	Ratio to failure probability of item A
Item A (reference)	1.54×10^{-5}	–
Case 0	6.91×10^{-6} ($\rho = 0.0$) 8.16×10^{-6} ($\rho = 0.3$) 9.86×10^{-6} ($\rho = 0.6$)	0.449 ($\rho = 0.0$) 0.530 ($\rho = 0.3$) 0.640 ($\rho = 0.6$)
Case S	2.54×10^{-6} ($\rho = 0.0$) 2.91×10^{-6} ($\rho = 0.3$) 3.28×10^{-6} ($\rho = 0.6$)	0.165 ($\rho = 0.0$) 0.189 ($\rho = 0.3$) 0.213 ($\rho = 0.6$)
Case T	2.08×10^{-6}	0.135

The annual failure probability of the system is numerically calculated to discuss the effectiveness of diversity in the natural period of items and additional seismic margins. The annual failure probability of the system, P_{fsys}, is calculated as follows:

$$P_{fsys} = \int_0^\infty f_S(s) F_{Sys}(s) \, ds \qquad (10)$$

where $f_s(s)$ is the probability density function of the annual maximum 5% damped spectral acceleration at 0.02 s, while $F_{Sys}(s)$ is the cumulative distribution function of the capacity of the system.

The results are tabulated in **Table 5**. For case 0, item B_0 is not so much effective to mitigate the consequences of accidents, because the failure probability of the system does not decrease <0.449–0.640 times as compared to that of item A. The failure probability of the system decreases 0.165–0.213 times as compared to that of item A for case S, and it decreases 0.14 times as compared to that of item A for case T. Both cases T and S are effective in mitigating the consequences of accidents, while case 0 is not because of the effects of common cause failure.

It still remains a room for discussion how this framework can be applied to the design of actual safety-critical facility. One of typical examples where the framework can be applied is the case when an emergency operations facility is additionally constructed in the vicinity of the facility. Whether a base-isolated structure is better than an earthquake-resistant structure for the emergency operations facility should be discussed not only by the performance of a single facility but also based on the performance of a group of facilities. The proposed framework can be used to discuss the latter case.

CONCLUSION

In this article, the sophistication of seismic design of safety-critical facilities was discussed from the viewpoint of seismic design of items that are important in mitigating the consequences of accidents to avoid cliff-edge effects. The proposed approach is considered to be related to an implementation of risk-informed and performance-based defense in depth.

First, it was pointed out that a strategy in mitigating the consequences of severe accidents to the point of near collapse is more important for safety-critical facilities than for basic facilities. Therefore, a basic framework for ensuring diversity in dynamic characteristics of items and providing additional seismic margin, such as a differentiation in classes of required seismic margins to each item based on its role, was proposed. This framework is meant to prevent a common cause failure and to avoid cliff-edge effects based on a risk-informed systems approach. The framework is proposed by utilizing the concepts of the FORM, probabilistic seismic hazard deaggregation, and the conditional mean spectrum. An appropriate combination of seismic margin and diversity was discussed to implement the defense-in-depth concept to seismic design based on the risk-informed approach. An example was demonstrated to prove that the proposed method was effective. The proposed method is considered to be useful because a defense-in-depth concept can be appropriately implemented under a wide range of seismic excitations.

Further applicability of the proposed method should be discussed using a more realistic system in future study. An actual safety-critical facility is composed of a large number of items and is much more complicated, although cases with two items are investigated in this article as a simplified example. Increasing the redundancy ensures higher level of safety, while total cost increases, including initial and maintenance costs. A framework of cost–benefit analysis should be developed to discuss how safe is safe enough. The effects of diversity in location of items in addition to diversity in dynamic characteristics are also needed to be discussed in the future study.

AUTHOR CONTRIBUTIONS

TI contributed to develop the framework and to conduct part of simulation study. YI contributed to conduct simulation. NS contributed to develop and elaborate the proposed framework of nuclear safety.

FUNDING

REFERENCES

Baker, J. W. (2011). Conditional mean spectrum: tool for ground motion selection. *J. Struct. Eng.* 137, 322–331. doi:10.1061/(ASCE)ST.1943-541X.0000215

Baker, J. W., and Jayaram, N. (2008). Correlation of spectral acceleration values from NGA ground motion models. *Earthq. Spectra* 4, 299–317. doi:10.1193/1.2857544

Bazzurro, P., and Cornell, C. A. (2002). "Vector-valued probabilistic seismic hazard analysis (VPSHA)," in *Proceedings of 7th U.S. National Conference on Earthquake Engineering* (Boston, MA).

Budnitz, R. J., Amico, P. J., Cornell, C. A., Hall, W. J., Kennedy, R. P., Reed, J. W., et al. (1985). *An Approach to the Quantification of Seismic Margins in Nuclear Power Plants, NUREG/CR-4334*. Washington, DC: Lawrence Livermore National Laboratory, U.S. Nuclear Regulatory Commission.

Haselton, C. B., Liel, A. B., Deierlein, G. G., Dean, B. S., and Chou, J. H. (2011). Seismic collapse safety of reinforced concrete buildings. I: assessment of ductile moment frames. *J. Struct. Eng.* 137, 481–491. doi:10.1061/(ASCE)ST.1943-541X.0000318

International Atomic Energy Agency. (1988). *Code on the Safety of Nuclear Power Plants: Siting, Safety Series, No. 50-C-S*. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency. (1996). *Defence in Depth in Nuclear Safety, INSAG-10*. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency. (2003). *Seismic Design and Qualification for Nuclear Power Plants, Safety Guide No. NS-G-1.6*. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency. (2006). *Fundamental Safety Principles, No. SF-1*. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency. (2016a). *Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (Rev. 1)*. Vienna: International Atomic Energy Agency.

International Atomic Energy Agency. (2016b). *Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791*. Vienna: International Atomic Energy Agency.

Itoi, T., Murakami, M., and Sekimura, N. (2015). Statistical equations of response spectra of crustal earthquake for assessment of multiple facilities seismic risk. *J. Jpn. Assoc. Earthq. Eng.* 15, 126–141; (in Japanese with English abstract). doi:10.5610/jaee.15.6_126

McGuire, R. K. (1995). Probabilistic seismic hazard analysis and design earthquakes – closing the loop. *Bull. Seismol. Soc. Am.* 85, 1275–1284.

Miyano, H., Takada, T., and Itoi, T. (2015). Tsunami resistant engineering for nuclear safety: (No.2) integrated risk-informed earthquake-tsunami protection framework for nuclear safety. *J. Atom. Energy Soc. Jpn.* 57, 639–645; (in Japanese).

Nuclear Regulatory Commission. (1997). *Regulatory Guide 1.165 Identification and Characterization of Seismic Sources and Determination of Safe Shutdown Earthquake Ground Motion (RG 1.165)*. Washington, DC: United States Nuclear Regulatory Commission.

Nuclear Regulatory Commission. (2007). *Regulatory Guide 1.208 A Performance-Based Approach to Define the Site-Specific Earthquake Ground Motion (RG 1.208)*. Washington, DC: United States Nuclear Regulatory Commission.

Rackwitz, R., and Fiessler, B. (1978). Structural reliability under combined random load sequences. *Comput. Struct.* 9, 489–494. doi:10.1016/0045-7949(78)90046-9

Shinozuka, M., Feng, M. Q., Lee, J., and Naganuma, T. (2000). Statistical analysis of fragility curve. *J. Eng. Mech.* 126, 1224–1231. doi:10.1061/(ASCE)0733-9399(2000)126:12(1287)

Structural Engineers Association of California. (1995). *Vision 2000 – A Framework for Performance-Based Design*. Sacramento, CA: Vision 2000 Committee.

Takada, T., Ochi, S., and Kanda, J. (2003). Basic study on determination of probabilistic controlling earthquakes. *J. Struct. Constr. Eng.* 68, 53–59; (in Japanese with English abstract). doi:10.3130/aijs.68.App53

United States Nuclear Regulatory Commission. (2012). *A Proposed Risk Management Regulatory Framework, NUREG-2150*. Washington, DC.

Wang, M., and Takada, T. (2005). Macrospatial correlation model of seismic ground motions. *Earthq. Spectra* 21, 1137–1156. doi:10.1193/1.2083887

Wang, M., Tanaka, K., and Takada, T. (2009). "Probabilistic seismic risk analysis for building portfolio," in *Proceeding of 10th International Conference on Structural Safety and Reliability, 13–17 September 2009* (Osaka, Japan: CRC Press Book).