

STRATEGIES FOR NUCLEAR STRUCTURES UNDER DEC, BDBA AND UNFORESEEN EVENTS

Yuxin Liu¹

¹ Senior Specialist Civil Engineer, Candu Energy Inc., a Member of AtkinsRéalis Company, 2251 Speakman Drive, Mississauga, L5K 1B2, ON, Canada (yuxin.liu@atkinsrealis.ca)

ABSTRACT

Nuclear power plants are designed to meet code requirements by ensuring structures, systems, and components (SSCs) can withstand design-basis conditions (DBC), including extreme environmental and accidental loads. Following accidents like Three-Mile Island and Chernobyl, loss-of-coolant accidents (LOCAs) became a critical design consideration. The 9/11 attacks necessitated addressing beyond design-basis accidents (BDBAs) such as aircraft impacts, while the Fukushima disaster prompted the inclusion of design extension conditions (DECs) to account for severe natural hazards. These events, often occurring unexpectedly, emphasize the need for comprehensive strategies to reduce failure probabilities, manage nuclear reactivity and heat removal, and ensure radioactive material containment, ultimately mitigating the impact of unforeseen BDBAs.

INTRODUCTION

Public trust in engineering relies on the delivery of safe and efficient products, within strict legal and regulatory boundaries. Design and construction processes must prioritize safety through adherence to codes, standards, and safety guidelines, encompassing comprehensive hazard identification, risk assessments, and rigorous quality control. Environmental responsibility is equally important, requiring the mitigation of air, water, and land pollution, and the integration of sustainability principles like energy efficiency and waste reduction. For critical infrastructure, particularly buildings and nuclear facilities, designs must ensure structural integrity to prevent progressive collapse (Liu, 2007), and implement robust containment measures to prevent radioactive releases, safeguarding both the environment and the public from severe accidents (USNRC–CNSC, 2025).

To ensure the operational integrity of nuclear power plant (NPP) designs, preventing accidents and mitigating their consequences, specific safety functions must be achieved under both design basis conditions (DBC) and design extension conditions (DEC). These functions, encompassing reactivity control, heat removal, radioactive material confinement, radiation shielding, and safety-critical parameter monitoring, are allocated across five defense-in-depth (DiD) levels, as outlined in regulatory guidelines (USNRC–CNSC, 2025). Design basis conditions, including normal operation, anticipated operational occurrences (AOOs), and design basis accidents (DBAs), are established to meet code requirements, primarily addressing DiD levels 1~3. For DiD levels 4 and 5, beyond design basis accidents (BDBAs) are considered to minimize radioactive releases and mitigate radiological consequences. These BDBA considerations require detailed analysis and assessment to inform complementary safety features and accident management guidelines. The plant states and DiD levels are closely linked to event classifications, determined through probabilistic studies and engineering judgment, and are correlated to annual frequency of occurrence per reactor (AFO): $1 > \text{AFO} \geq 10^{-2}$, $10^{-2} > \text{AFO} \geq 10^{-5}$, and $10^{-5} > \text{AFO}$ for AOOs, DBAs, DECs /BDBAs, respectively (USNRC–CNSC, 2025). Notably, for design basis tornadoes, AFO can be as low as 10^{-7} (USNRC, 2007). Reducing AFO is a critical strategy for mitigating radiological consequences.

Table 1 CNSC plant states considered as design envelope.

Operational states		Accident conditions		
Normal operation, Level 1	Anticipated operational occurrence (AOO), Level 2	Design basis accident (DBA), Level 3	Beyond design basis accidents	
			Design extension conditions (DEC)	Practically eliminated conditions
			No severe fuel degradation	Severe accidents
Design basis		Design extension (DE), Level 4	Not considered as DE, Level 5	
Reducing frequency of occurrence →				

The application of relaxed codes and standards acceptance criteria is permissible for DEC assessments, aiming to prevent severe fuel degradation. However, this approach is insufficient for unforeseen BDBAs, which lack a defined lower bound AFO. This challenge necessitates the development of specialized strategies to effectively address these events.

UNFORESEEN EVENTS DURING DESIGN

Foreseen event failures are preventable, as their causes are identifiable. Adherence to code requirements and quality assurance protocols during design, construction, and operation can mitigate such failures. Design flaws, including inappropriate site selection, system misuse, material selection errors, omitted load cases, inaccurate analyses, and ambiguous design communication, significantly contribute to these failures. Conversely, unforeseen failures, caused by unknown and unexpected events or loads, may be unavoidable, even when structures, systems, and components (SSCs) are built to code.

Typical BDBA Events in NPPs

In 1979, the Three Mile Island Unit 2 (TMI-2) reactor in Pennsylvania suffered a partial core meltdown following a cooling system failure after roughly one year of operation, and the core damage is shown in Figure 1(a) (Högberg, 2013). The incident sequence began with a stuck-open pressurizer relief valve, causing a continuous loss of coolant from the reactor's primary system. Operators, misinterpreting the pressurizer water level as indicative of sufficient core coverage, ceased cooling water injection, leading to core dryout and overheating. Over two hours elapsed before the block valve, in series with the stuck-open valve, was closed, and recovery efforts commenced. A hydrogen burn within the containment generated a pressure spike of approximately 0.2 MPa, which remained within the containment's design basis. While a minor release of radioactive gas occurred several days post-accident, radiation doses to local residents were negligible, remaining below background levels. The accident's root causes were attributed to a confluence of equipment malfunctions, design-related issues, and operator errors.

In 1986, the Chernobyl nuclear power plant in Ukraine experienced a catastrophic accident. Operators, conducting a test at low power, destabilized the reactor by violating prescribed operating limits and disabling safety systems. Activating the reactor shutdown button initiated a rapid power surge, leading to the explosive rupture of numerous fuel channels. The resulting steam and gas release overpressurized the core cavity, lifting and displacing the 1000-ton reactor lid and control rods. A subsequent explosion, likely involving hydrogen, completely destroyed the reactor, and the damage of reactor building is shown in Figure 1(b). Evaporated fuel and fuel fragments were ejected high into the atmosphere, and a graphite fire burned for approximately ten days. As identified by Högberg (2013), the

accident's root causes stemmed from significant design flaws (shutdown system, containment capacity), inadequate safety analysis, insufficient independent safety review, operator errors resulting from a lack of safety awareness, and a pervasive lack of safety culture within the political and organizational structures at both national and local levels.

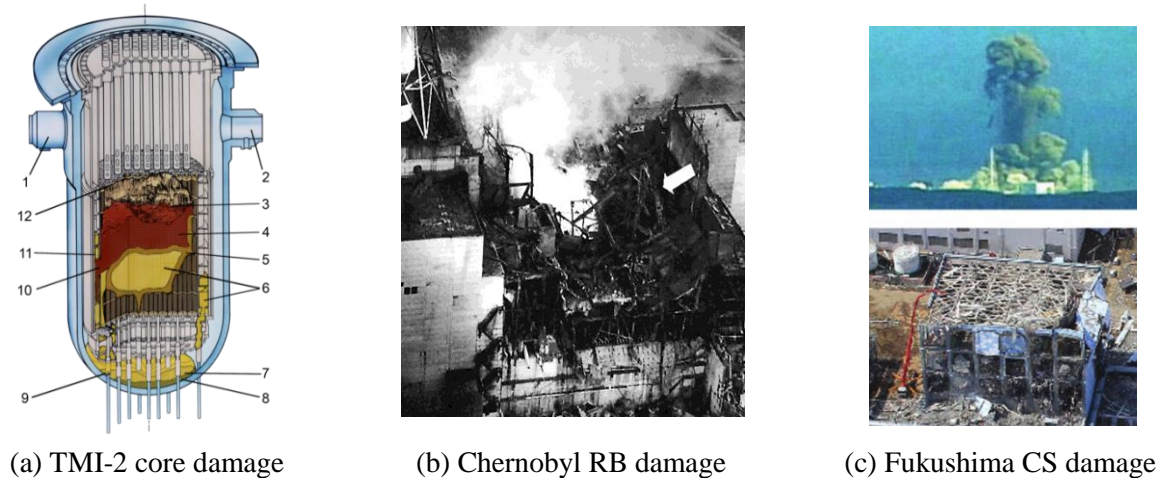


Figure 1. Failure of nuclear facilities caused by unforeseen BDBAs.

In 2011, the Fukushima Daiichi Nuclear Power Station in Japan, operating six boiling water reactors commissioned in the 1970s, experienced a severe accident. A magnitude 9.0 earthquake centered approximately 200 km offshore, impacted units 1-3 (operating) and 4-6 (shutdown). The earthquake triggered automatic shutdown of operating reactors, with peak ground acceleration reaching 0.56g (22% above the design value of 0.46g). While emergency diesel generators initially provided power after the earthquake disrupted external power, a subsequent 14m tsunami (146% above the 5.7m design basis) flooded reactor and turbine buildings. This flooding led to the failure of emergency systems, resulting in the loss of core cooling in units 1~3. Overheating and probable core meltdowns occurred, followed by hydrogen explosions that destroyed containment structures as shown in Figure 1(c), releasing substantial amounts of fission products. The root causes were attributed to design deficiencies in structures, systems, and components (SSCs) that failed to withstand the tsunami and subsequent explosions (Högberg, 2013).

The comprehensive analysis of the TMI-2, Chernobyl, and Fukushima accidents (Högberg, 2013) identifies recurring root causes: flaws in the design of structures, systems, and components (SSCs) vital for safety, insufficient safety management practices, and a deficient safety culture permeating both the nuclear industry and regulatory bodies. These systemic issues demand careful consideration in subsequent designs to prevent similar incidents. Notably, the profound consequences of these accidents were largely unpredictable before their occurrence, classifying them as unforeseen beyond design basis accidents (BDBAs). Given the potential for devastating outcomes from BDBAs, design methodologies must incorporate robust strategies to constrain radioactive releases and safeguard the environment and public health.

BDBA Events in Civil Engineering

In civil engineering, beyond design basis accident (BDBA) events are considered abnormal loading conditions. The 1968 Ronan Point accident, involving a partial collapse of a 22-story building shown in Figure 2(a), exemplifies this. A gas explosion in an 18th-floor apartment blew out an exterior wall panel, initiating a progressive collapse. The resulting reduced support caused the roof to fail, and the falling

debris triggered a chain reaction, leading to the collapse of floors nearly to ground level. As a result of this accident, design codes now require consideration of pressure loading from gas explosions to prevent progressive collapse (Liu, 2007).

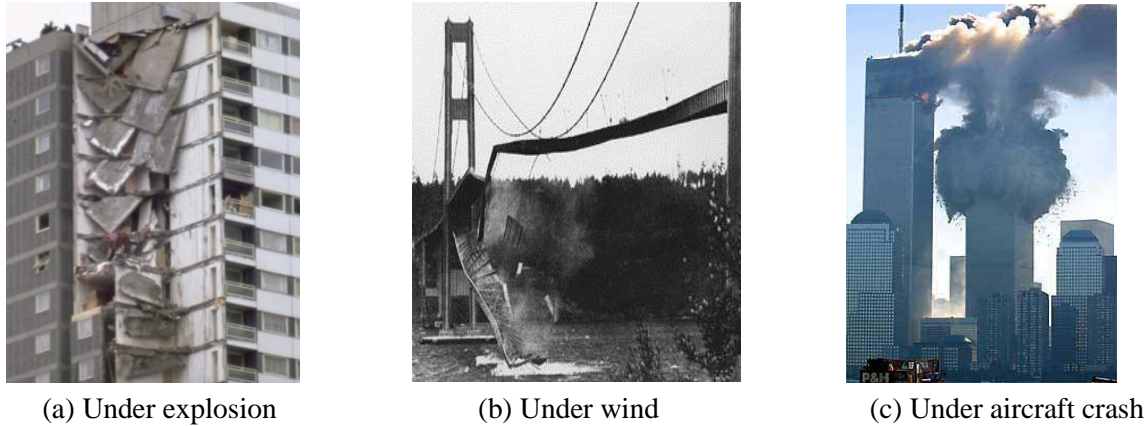


Figure 2. Structural collapses caused by unforeseen loading events.

The Tacoma Narrows Bridge, notable for its innovative use of plate girders to support the roadway, revealed critical design flaws shortly after its completion in late June 1940. It displayed alarming oscillations and buckling under relatively light wind conditions (Wikipedia, 2025). The bridge's dramatic failure, characterized by an unprecedented twisting mode at a wind speed of 64 km/h, illustrated in Figure 2(b), had a profound impact on bridge engineering. This event catalysed significant research into bridge aerodynamics and the integration of dynamic and modal analyses into design practices, leading to the adoption of wider decks, stiffening struts, and wind-permeable structures.

The catastrophic collapse of the World Trade Center twin towers in 2001, illustrated in Figure 2(c), triggered by the impact of two aircraft, underscored the vulnerability of tall structures to extreme events. A comprehensive investigation by the United States Federal Emergency Management Agency (FEMA, 2002) identified a distinct sequence of loading events contributing to the failure: (i) the initial aircraft impacts, which severed critical elements of the exterior steel superstructure, causing substantial localized damage; (ii) the ensuing intense fires, fuelled by jet fuel and combustible office materials, which progressively weakened the structural integrity of the damaged building; and (iii) the cascading impact of falling debris, resulting from the progressive collapse, which overwhelmed the remaining structural capacity. The FEMA report noted that the structural redundancy of the towers initially mitigated immediate collapse following the impacts (i), with load redistribution through the exterior wall frame. However, the prolonged fires (ii) significantly reduced the structural resistance, and the subsequent debris impact (iii) caused a progressive failure (Figure 2(c)). This event highlighted the urgent need for research into progressive collapse under abnormal loading conditions. A significant consequence for the nuclear industry is the US Nuclear Regulatory Commission's (USNRC, 2011) requirement for new NPPs to incorporate design considerations for the BDBA events of large commercial aircraft crashes.

SOCIAL RESPONSE TO ENGINEERING BDBA CONSEQUENCES

The inevitable occurrence of engineering facility failures, stemming from shortcomings in design, construction, and operation, triggers a multifaceted social response. This response is characterized by accountability demands, proactive efforts to prevent recurrence, an increased focus on safety and design

quality, legal and ethical scrutiny, and the implementation of stringent regulatory frameworks for engineering practice.

Code Requirements

To mitigate catastrophic facility failures and damage to engineered products, engineers, constructors, operators, owners, and regulators must adhere to relevant requirements, addressing common engineering errors such as inadequate product design, substandard material usage, flawed construction techniques, non-compliance with codes, standards, and regulations, neglect of aging and environmental impacts, and inadequate maintenance. Code violations carry severe professional repercussions. For example, the Hammurabi Building Code (Admin, 2023), dating to approximately 1772 BC, stipulated stringent penalties for construction failures:

“229 – If a builder builds a house for someone, and does not construct it properly, and the house falls in and kills its owner, then that builder shall be put to death.

230 – If it kills the son of the owner, the son of that builder shall be put to death.

231 – If it kills a slave of the owner, then he shall pay, slave for slave, to the owner of the house.

232 – If it ruins goods, he shall make compensation for those goods, and inasmuch as he did not construct properly this house which he built and it fell, he shall re-erect the house from his own means.

233 – If a builder builds a house for someone, even though it is not yet complete; if then the walls seem toppling, the builder must make the walls solid from his own means.”

While these clauses may not be directly applicable to contemporary engineering practice, they underscore the imperative to perform work diligently to prevent catastrophic damage. Engineering accidents often trigger legal investigations and lawsuits, exposing engineers and companies to penalties for negligence or non-compliance with technical codes, standards, and regulatory requirements. Deficient communication can lead to unanalysed and unapproved design modifications, contributing to engineering failures. Engineering professionals are ethically obligated to safeguard public safety, health, and welfare, and breaches of this duty can result in severe consequences.

Lawsuit Cases against Unforeseen BDBAs

The prediction of earthquake epicentres and intensities remains a significant challenge within earthquake engineering, given the current limitations of instrumentation and scientific knowledge. This difficulty was poignantly illustrated by the 2009 L'Aquila earthquake (magnitude 6.3), which resulted in devastating casualties and structural damage (Figure 3(a)).



(a) L'Aquila building collapse



(b) Rally against TEPCO executive

Figure 3. Lawsuit cases against consequences of unforeseen events.

The subsequent legal actions, which alleged that scientists provided inaccurate reassurances to the public regarding the absence of a major earthquake, sparked international debate. While a local court initially found seven scientists and experts guilty of manslaughter, this verdict was widely criticized, with the American Association for the Advancement of Science denouncing the charges as "unfair and naive." Ultimately, the Italian Supreme Court overturned the majority of these convictions in 2015, and related charges against other implicated officials were also dropped. Cartlidge (2016) reported that this protracted legal battle, which spanned seven years, highlighted the ethical and legal complexities faced by scientists and engineers when dealing with natural disasters, which can be categorized as BDBA event. The case illuminates the risk that professional experts face when trying to predict the unpredictable.

The 2011 Fukushima Daiichi nuclear accident, resulting in the worst nuclear disaster since Chernobyl and the forced evacuation of hundreds of thousands, initiated significant legal action. Shareholders of Tokyo Electric Power Company (TEPCO) filed a lawsuit in 2012, seeking to hold former TEPCO executives accountable for the disaster. In July 2022, a Tokyo district court ruled that three former executives, including the former TEPCO President, were liable for 13 trillion yen (\$95 billion) in damages. However, this decision was appealed, and the Tokyo High Court subsequently acquitted the executives of manslaughter in relation to the triple reactor meltdown (Figure 3(b)). The appeal focused on the central question of whether the tsunami, which caused the plant's destruction, could have been predicted, and consequently, whether the accident could have been prevented. The High Court's ruling overturned a 2019 Tokyo district court judgment that had also found the executives not guilty of professional negligence, based on the argument that the tsunami's magnitude was unforeseeable (Ogura, 2023).

Severe engineering accidents, particularly those resulting in injuries or fatalities, garner significant media attention, subjecting engineers, companies, and regulatory bodies to intense public scrutiny. This scrutiny often involves questioning design choices and demanding accountability for failures. Notable incidents, such as those at Three Mile Island (TMI), Chernobyl, and Fukushima, have catalysed calls for enhanced safety protocols, stricter regulations, and improved training for engineers and operators, emphasizing the prioritization of safety and ethical considerations in their work. Engineering professionals bear a fundamental duty to protect public well-being, ensuring that their designs are not only innovative but also safe and ethically sound. Failure analysis and investigation are critical for identifying the root causes of engineering failures and implementing preventative measures. Learning from past failures is essential for advancing safety standards and engineering practices. Revising engineering codes, standards, and regulatory safety guidelines based on root cause analyses from previous disasters can effectively mitigate and prevent future failures.

ENGINEERING STRATEGIES AGAINST UNFORESEEN BDBAS

Engineers and operators may face professional license revocation, fines, criminal charges, and imprisonment for accidents, especially those resulting from negligence or failure to adhere to professional standards that cause harm or death. If engineering professionals rigorously comply with codes, standards, regulatory requirements, and quality assurance protocols, and a failure occurs due to unforeseen factors, they are generally not held liable for damages or subject to criminal penalties, particularly within the nuclear industry. Nevertheless, science and engineering disciplines must develop robust strategies to mitigate the consequences of unforeseen accidents.

Reducing Uncertainty

Failures resulting from foreseen events, such as Anticipated Operational Occurrences (AOOs), Design Basis Accidents (DBAs), and even Design Extension Conditions (DECs) in nuclear power plants, are

generally preventable. This is because the causal factors are known, and Structures, Systems, and Components (SSCs) are designed and constructed in accordance with established design codes and standards. Rigorous adherence to code requirements and quality assurance protocols during design, construction, and operation can mitigate these failures. However, failures stemming from unforeseen events due to design input uncertainties may be unavoidable, as the causal factors are often unknown and influenced by extreme, uncertain variables. For instance, the Fukushima Daiichi nuclear power plant was designed to withstand specific earthquake intensity but was overwhelmed by the subsequent tsunami. The plant's units 1 to 3 were safely shut down as designed upon initial earthquake detection. The earthquake's peak horizontal accelerations reached 0.56g, exceeding the design basis of 0.46g by approximately 27%. While this discrepancy may not have directly caused plant damage, the ensuing tsunami, with wave heights reaching approximately 14 meters above sea level, significantly exceeded the plant's design basis of 4 meters, later increased to 5.7m (Figure 4(a)) (Högberg, 2013).

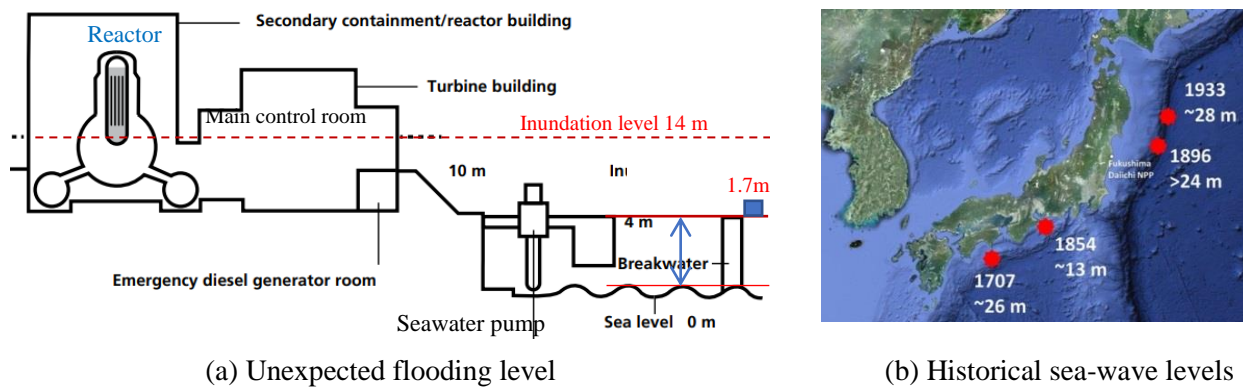


Figure 4. Unforeseen tsunami level affecting Fukushima Daiichi plant (Högberg, 2013).

The flooding of the reactor and turbine buildings resulted in the failure of emergency diesel generators, power distribution systems, and control equipment, leading to a loss of core cooling and subsequent core melt damage in units 1 to 3. In contrast, units 5 and 6, located on higher ground, maintained emergency diesel functionality, ensuring adequate core cooling. As shown in Figure 4(b) and detailed in Table 2, historical tsunami height data from 1704 to 1933 in the vicinity of the Fukushima Daiichi plant indicates a high mean tsunami height of 22.8m, with a standard deviation of 6.7 meters. If the plant's design had incorporated this historical data, including one standard deviation to account for uncertainty, a design basis tsunami wave height of 29.5m would have been considered. Therefore, the original design height of 4m, later increased to 5.7m, significantly underestimated the potential flooding risk compared to the actual 14-meter inundation, which was itself less than the lower bound of 16.1m (22.8 - 6.7m).

Table 2: Data of Tsunami wave levels related to Fukushima Daiichi plant design.

Year/term	1707	1854	1896	1933	Mean	SD	Designed	Updated	Occurred
Height (m)	26	13	24	28	22.8	6.7	4	5.7	14

As illustrated by the preceding example, thorough investigations are essential to obtain reliable design inputs, facilitating informed decision-making and reducing uncertainty, thereby mitigating failure consequences. However, when design inputs fail to accurately predict potential operational or occupancy conditions, alternative mitigation strategies must be developed to prevent catastrophic failures.

Reducing Failure Probability

As indicated in Table 1, for DiD Level 5, reducing AFOs is a practical strategy to mitigate Beyond Design Basis Accident (BDBA) consequences. In nuclear engineering, BDBA events encompass extreme conditions such as temperature, pressure, missile impact, flooding, tornadoes, and high winds. Pressure loading can arise from explosions within service systems (e.g., natural gas and steam), stored gases and liquids (butane, propane, oxygen, gasoline), hazardous materials in transit, or intentional acts such as bombing. Additionally, sonic booms can induce pressure loading on structures. Natural phenomena, such as tornadoes and hurricanes, also generate significant pressure loading. Impact loading can result from ground vehicle collisions, aircraft crashes, missile or military weapon impacts, and structural failures of adjacent buildings or falling debris. Further loading scenarios include malfunctions within water or other service systems, and debris generated from external incidents.

Accurate determination of a system's failure probability is essential for effective risk assessment and frequency reduction. In nuclear engineering, probabilistic risk assessment (PRA) is a widely employed methodology for this purpose. Fault tree analysis (FTA) is utilized to identify the root causes of system failures and to compute the probability of failure events based on individual component failure probabilities. Subsequently, event tree analysis (ETA) is conducted to evaluate potential outcomes following an initiating event, considering various failure pathways. Statistical, Bayesian, Markov, reliability, and Monte Carlo analyses can also be applied, depending on system complexity, data availability, and desired accuracy. This study illustrates the reliability-based stable configuration approach for calculating failure probability. Based on the stable configuration method, the failure probability P_F of a system due to BDBA events is given by (Bennett, 1988):

$$P_F = 1 - \exp\left[-t \sum_{k=1}^m v_k P_{Fk}\right] \quad (1)$$

in which t is the design lifetime of a system under potential m BDBA events. For each BDBA event k , v_k is its mean rate of occurrence; and P_{Fk} is the corresponding failure probability. Equation 1 is based on the occurrence of an event following an independent Poisson process. As the BDBA interaction frequency is extremely low, it is reasonably considered that there are no simultaneous occurrences of BDBA events. The stable configuration approach of system reliability is applied for calculating failure probability P_{Fk} ,

$$P_{Fk}(N \geq j) = P\left(\bigcap_{i=1}^I C_{ki}\right) \quad (2)$$

where N is the number of components that have failed related to I cuts, and C_{ki} is the failure probability of cut i - i . An SSC system shown in Figure 5(a) is used for illustrating the calculation, where components 1 to 4 are considered vulnerable; components 5 to 8 are less vulnerable; and components 9 and 10 are rigid boundary not affected by any BDBA. The following two BDBAs are assumed to cause intermediate damage: internal explosion-generated damage U_1 with annual probability 1.8×10^{-5} , and external missile impact U_2 with annual probability 6×10^{-4} .

Corresponding to the system under U_1 in Figure 5(a), a graph of the possible sequences of failure is shown in Figure 5(b). BDBA U_1 causes the failure of component 3 to have a Cut a-a, and then failure of components 1, 2, 4 might fail that is related to Cut b-b. With the progressive failure of component 1 after Cut b-b, an interactive failure may happen as Cut c-c shown in Figure 5 (b). With considering all the possible combined cuts, the stable configuration approach is followed for calculating the failure probability. Assume the design life for this system is 50 years, and other values of means, standard

deviations, and variable correlation factors for system remaining unchanged, the failure probability occurring during the system lifetime based on Equations 1 and 2 is given by:

$$P_F = 1 - \exp[-50\{1.8 \times 10^{-5}(0.031 + 0.065 + 0.017 + 0.0038) + 6 \times 10^{-4} \times 0.0026\}] = 1.83 \times 10^{-4}$$

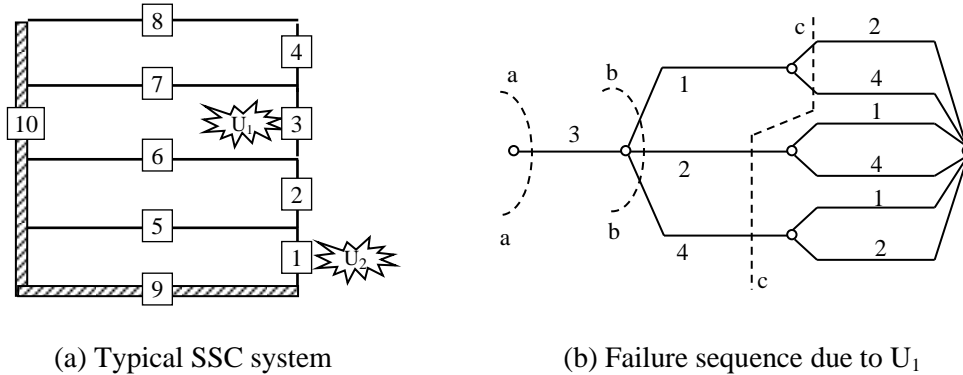


Figure 5. Failure modelling and analysis of a system subject to unforeseen BDBAs.

The calculated failure probability above for the safety system from all causes is lower than 1.0×10^{-3} as required by CNSC (USNRC–CNSC, 2025). When the design life is changed to 100 years, the internal explosion U_1 annual probability is changed as 1×10^{-5} , and external missile impact U_2 annual probability is changed to 1×10^{-4} , which are considered two BDBAs, and the system properties remain unchanged, the calculated failure probability is 3.77×10^{-5} , which is even lower. Note that this example is similar to the Example 1 in the research of Bennett (1988), and more detailed system properties and calculations can be found in that paper. In general, the demand and capacity for a cut may be obtained by a probabilistic analysis, and then stable configuration approach is followed to calculate failure probability. In general, this approach may be applied to estimate the sum of frequencies of all BDBA event sequences that can lead to significant core degradation to be less than 10^{-5} per reactor year, and to any release to the environment with long-term relocation of the population to be less than 10^{-6} per reactor year.

Goal-Based Design

Minimizing AFO or failure probability is a reasonably practicable strategy for designing NPPs to withstand BDBAs. This approach aligns with the principle of reducing risk to as low as reasonably practicable to enhance safety. Even when AFOs cannot be completely eliminated, and the sum of frequencies of all unforeseen BDBA event sequences is in the range of 0 to 10^{-6} per reactor year, a goal-based design (GBD) strategy can facilitate achieving the following critical safety objectives:

- Reactor shutdown and maintained shutdown state
- Decay heat removal from the reactor core and fuel pool
- Containment of radioactive materials
- Maintaining the functionality of plant monitoring and control systems

The GBD in NPPs prioritizes achieving critical safety objectives by shifting from simple feature implementation to ensuring effective minimization of radiation exposure to workers, the public, and the environment, particularly during DBCs, DEC, and BDBAs. A robust DiD strategy is essential, involving multiple layers of safety systems to prevent core damage and radioactive releases, and to mitigate consequences, especially during unforeseen BDBAs. Preventing BDBAs through strong physical security, protecting the plant from external threats and nuclear material diversion, is a fundamental approach. However, when BDBAs are unavoidable, engineered safety systems and operational procedures must be

in place for prevention and mitigation. Emphasizing passive safety systems, which rely on natural forces, enhances safety by reducing reliance on active, power-dependent systems.

Various methodologies, including structural integrity design, localized resistance, and alternate load paths (Liu, 2007), can be implemented to mitigate BDBA failures. When BDBA avoidance is impractical, as exemplified by the Fukushima plant's foundation level being below the 14m inundation height, an alternative strategy focusing on preventing radioactive material release to the environment and public, regardless of the BDBA, is essential. This GBD approach provides a practical solution for reactivity control of nuclear fuel, heat removal from the reactor core and spent fuel pool, and radioactive material containment. Implementing this design requires localized resistance and alternate load paths to ensure the functionality of safety-related SSCs under unforeseen BDBA conditions, while minimizing AFOs. Specifically, critical monitoring, control, and emergency equipment can be isolated from BDBA-induced extreme temperature, pressure, fire, and flooding to achieve the safety goal.

CONCLUSION

To prevent future disasters, engineers must learn from past failures like TMI, Chernobyl, and Fukushima by designing for greater resilience. This involves a proactive shift towards reducing uncertainty, minimizing failure probability, and implementing goal-based design. Practical measures, such as alternate load paths and rigorous frequency analyses, are essential. In the face of unpredictable BDBAs, especially those involving extreme conditions like temperature, pressure, fire, flooding, seismic activity, missile impact, and aircraft crashes, isolation strategies are crucial for ensuring the continued safety and reliability of critical systems.

REFERENCES

- Admin, (2023), Building Codes, <https://engineeringdesignresources.com/building-codes/>.
- Carlidge, E. (2016). Seven-year legal saga ends as Italian official is cleared of manslaughter in earthquake trial, Science Adviser.
- Bennett, R. M. (1988). Formulations for probability of progressive collapse, Structural Safety, Volume 5, Issue 1, Pages 67-77.
- FEMA. (2002). World Trade Center building performance study: Data collection, preliminary observations and recommendation. FEMA-403, New York, N.Y. USA.
- Högberg, L. (2013). Root Causes and Impacts of Severe Accidents at Large Nuclear Power Plants. AMBIO, 42, 267–284.
- INPO. (2021). Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station, Exhibit 3, Revision 0, INPO 11-005, Special Report.
- Ogura, J. et.al. (2023). Tokyo High Court acquits three former TEPCO executives over 2011 Fukushima nuclear accident: NHK, CNN.
- Liu, Y. (2007). *Progressive-failure analysis of steel building structures under abnormal loads*, Ph.D. Thesis. Waterloo (ON, Canada): University of Waterloo.
- USNRC. (2007). “Design-Basis Tornado and Tornado Missiles for Nuclear Power Plants,” RG 1.76, 2007, Washington, DC., United States of America.
- USNRC. (2011). *Guidance for the assessment of beyond-design-basis aircraft impacts*, RG 1.217, Washington, DC., United States of America.
- Wikipedia. (2025 accessed). Tacoma Narrows Bridge (1940).
- USNRC–CNSC. (2025). Concerning Classification and Assignment of Engineering Design Rules to Structures, Systems, and Components, Memorandum of Cooperation JOINT REPORT.