DOI: https://doi.org/10.15407/pmach2025.04.006

UDC 621.039

OPERATIONAL PROBABILISTIC SAFETY ANALYSIS OF A NUCLEAR POWER PLANT OPERATING UNDER EXTREME CONDITIONS

Andrii O. Kostikov
kostikov@ipmach.kharkov.ua
ORCID: 0000-0001-6076-1942

Leonid I. Zevin

Anatolii Pidhornyi Institute of Power Machines and Systems of NAS of Ukraine,
2/10, Komunalnykiv str., Kharkiv, 61046, Ukraine

The problem of rapid risk assessment for nuclear power plant operation under extreme conditions, which may significantly affect nuclear and radiation safety, is considered. Based on a probabilistic safety analysis approach, a methodology has been developed to evaluate accident risk. Its application enables plant personnel to quickly make decisions on the need to reduce the reactor power or shut down the power unit in the event of circumstances that could seriously compromise operational safety. A formula for calculating the maximum permissible reactor power at which the plant can continue to operate in extreme conditions is obtained. It is shown that in cases of events posing substantial risk and potentially leading to accidents, shutting down the unit is advisable, as safety limits may otherwise be exceeded.

Keywords: *nuclear power plant, probabilistic safety analysis, maximum allowable reactor power, reactor shutdown.*

Introduction

According to current regulatory documents in the field of nuclear and radiation safety of nuclear facilities [1], the methodology for safety analysis of nuclear power plants is based, among other aspects, on a probabilistic approach. At the same time, generally accepted safety criteria establish maximum permissible values of the accident probability P [2]. In the case of a design basis accident, the following condition must be met

$$P \le P^*; \quad P^* = \frac{10^{-5} \ldots 10^{-4}}{\text{reactor} \times \text{year}},$$

and for a beyond design basis accident –

$$P \le P^*; \quad P^* = \frac{10^{-8} \ldots 10^{-7}}{\text{reactor} \times \text{year}}.$$

The history of radiation incidents and accidents has shown [3] that their cause is usually the human factor, equipment failure or the impact of natural events that were not foreseen by the design (for example, the earthquake and tsunami that led to the Fukushima nuclear accident). At the same time, humanity is now facing a new challenge, namely the existence of a significant risk of an accident at a civilian nuclear facility as a result of hostilities in the area of its location, or deliberate nuclear terrorism. Unfortunately, examples of this already exist. This includes the deliberate destruction of distribution substations leading to emergency shutdowns of nuclear power plant units, the shelling of the South Ukraine NPP that caused damage to a building and disabled auxiliary equipment, and the transformation of the Zaporizhzhia NPP site into a de facto military base with heavy weaponry and ammunition depots located in close proximity to reactor units. Thus, the problem of operational risk assessment of nuclear power plant operation in extreme conditions is very significant. We add that its analysis under certain conditions consists of two main tasks: calculating the probability of accidents and determining their consequences. The product of these quantities can be considered as a quantitative assessment of risk.

The probability of accidents is usually calculated using the event scheme of probability theory in the form of graph-analytical methods of the event "tree" and the failure "tree" [4]. The general concept of operational risk assessment of nuclear power plant operation is set out in [5]. At the same time, the specified paper lacks information on how to develop probabilistic models. By the way, such models should allow calculations to be made in real time so that the automation and/or personnel of the plant can promptly respond to the occurrence of extreme operating conditions.

Thus, the problem of developing a methodology for operational probabilistic analysis of nuclear power plant operation safety is relevant.

Methodology for calculating the accident probability

We will consider the nuclear power plant unit as an object consisting of two structures. The first one – $\{S_1, S_2, \ldots, S_M\}$ – is a set of safety systems which function is to prevent accidents or limit their consequences. The second one – $\{D_1, D_2, \ldots, D_N\}$ – is normal operation systems and other auxiliary systems.

We will assume that each system D_n, n=1, 2, …, N and every system S_m, m=1, 2, …, M can be in one of two states: "operable" or "failed". We will also assume that the safety systems S_m are independent of each other and of systems D_n.

Let's introduce events A_k, k=1, 2, …, K, each of which will characterize a certain state of the set of safety systems $\{S_1, S_2, \ldots, S_M\}$ regarding their operability. Since each safety system can only be in one of two states ("operable" or "failed"), then, obviously, the number of all unique possible events that reflect the state of the set of safety systems will be $K=2^M$. Events A_k can be arranged in different ways, but for the purposes of the following discussion, their order is not important.

We denote the probability that the safety system S_m is in the "operable" state, as p_m, m=1, 2, …, M. Obviously, in this case, the probability that the safety system S_m is in the "failed" state will be $1–p_m$. Since the systems S_m are independent of each other, the probability of the event A_k is defined as the product of the probabilities that each of the systems S_m is in the state corresponding to the event A_k, i.e.

$$P(A_k) = q_1 \cdot q_2 \cdot \ldots \; q_M,$$

where $q_m=p_m$, if at the event A_k the system S_m is in the "operable" state, and $q_m=1–p_m$, if at the event A_k the system S_m is in the "failed" state.

Since none of the safety systems S_m can be in the "operable" and "failed" states at the same time, then all events A_k, k=1, 2, …, K are pairwise incompatible, i.e. they form a complete group of events and the sum of their probabilities is equal to one

$$P(A_1) + P(A_2) + \ldots + P(A_k) = 1.$$

Let's introduce the following notation: $h_n(D_n)$, n=1, 2, …, N – an event that results in a system D_n failure; $P(h_n)$, n=1, 2, …, N – probability of such an event; E_n – the corresponding accident at the NPP power unit initiated by this event.

In addition to failures of systems that are part of the power unit, the causes of accidents can be external influences, such as abnormal events in the Unified Energy System, leading to an emergency shutdown of the NPP from it, accidents at distribution system facilities, terrorist attacks directly on the NPP or on other energy infrastructure facilities related to its operation, military operations in the immediate vicinity of the plant, extreme natural phenomena (earthquakes, tsunamis), etc.

To describe them, we will use similar terminology and mathematical apparatus. Let's set that X_μ, μ=1, 2, …, μ^* – a set of external systems (or factors) that can affect the operation of a power unit.

We introduce the following notations: $H_\mu(X_\mu)$, μ=1, 2, …, μ^* – an event that consists in the failure of an external system (or the appearance of an external negative factor) X_μ; $P(H_\mu)$, μ = 1, 2, …, μ^* – probability of such an event; E_μ – the corresponding accident at the NPP power unit initiated by this event.

We will assume that all events A_k, k=1, 2, …, K, h_n, n=1, 2, …, N, H_μ, μ = 1, 2, …, μ^* are independent due to the structural architecture of the power unit. Since both the failure of normal operation systems and external influences can lead to an accident, in order to reduce the calculations, we will not make a distinction between them further, and any event, either h_n n=1, 2, …, N, or H_μ μ=1, 2, …, μ^* will be denoted as d_U, and the corresponding accident – as E_U.

To prevent accidents E_U, in the event of d_U, the latter one is parried by the safety systems of the power unit. Since these systems in the event of d_U can be in only one of the set of states corresponding to the events A_k, k=1, 2, …, K, only those safety systems that are operational for this current event A_k will be operated. Let $P(E_U \backslash A_k)$ be the conditional probability of an accident E_U in the event A_k. Then, according to the formula of total probability, the probability of an accident E_U due to an event d_U can be expressed as

$$P(d_U \cdot E_U) = p(d_U) \cdot \sum_{k=1}^{K} P(A_k) \cdot P(E_U \setminus A_k)\,. \tag{1}$$

Accident risk assessment

In addition to the probability of an accident, when assessing its risk, quantitative indicators of its consequences are also considered, in particular, the costs of eliminating these consequences. Such quantitative indicators depend on many factors, including the reactor power at which it was operating at the time of the accident. Usually, the lower the reactor power is, the smaller the magnitude of the consequences of the accident, in particular, the monetary equivalent of the costs of post-accident restoration of the power unit will be.

Let τ be the moment of time when the initiating event d_U occurred. After this moment, the safety systems work out a certain period of time $[\tau, \tau_1]$, which may allow to maintain the magnitude of the accident risk at an acceptable level during it and not to stop the operation of the power unit, reducing only its power if necessary. If the risk is high, the operator can put the unit into a shutdown state.

Let $c_U(\theta)$ be the magnitude of the costs that can be used to eliminate the consequences of the accident during time θ, and $c_{\max}(\theta)$ be the maximum value of the costs that can be used. We consider the magnitude of the accident consequences E_U, which in dimensionless form is written as

$$g_U(\theta) = \frac{c_U(\theta)}{c_{\max}(\theta)} \cdot \frac{V_U(\tau)}{W_0}, \tag{2}$$

where $V_U(\tau)$ is the reactor power at the moment of the initiating event d_U; W_0 is the nominal reactor power.

Then the accident risk can be written as the product of the consequences times its probability

$$R_U(\theta,\tau) = \frac{c_U(\theta)}{c_{\max}(\theta)} \cdot \frac{V_U(\tau)}{W_0} \cdot p(d_U(\tau)) \cdot P(E_U(\tau)) \cdot \frac{1}{\text{reactor} \times \text{year}}. \tag{3}$$

where $p(d_U(\tau))$ is the probability of the initiating event d_U, which can occur in time $[0, \tau]$; $P(E_U(\tau))$ – probability of an accident due to the event d_U.

Since the probability of any design basis or beyond design basis accident should not exceed the value P^*, that is,

$$p(d_U(\tau)) \cdot P(E_U(\tau)) \le P^* \cdot \frac{1}{\text{reactor} \times \text{year}}, \tag{4}$$

then from (3) we obtain

$$R_U(\theta,\tau) \le \frac{c_U(\theta)}{c_{\max}(\theta)} \cdot \frac{V_U(\tau)}{W_0} \cdot P^* \cdot \frac{1}{\text{reactor} \times \text{year}}. \tag{5}$$

Inequality (5) has expert status, since the quantities P^*, $c_U(\theta)$, $c_{\max}(\theta)$ are determined by experts.

If the power unit operates at nominal mode, i.e.

$$V_U(\tau) = W_0, \tag{6}$$

then (5) gives an estimate for the risk

$$R_U(\theta,\tau) \le \frac{c_U(\theta)}{c_{\max}(\theta)} \cdot P^* = \gamma \cdot P^* \cdot \frac{1}{\text{reactor} \times \text{year}}. \tag{7}$$

where $\gamma = \dfrac{c_U(\theta)}{c_{\max}(\theta)}$.

Determination of the maximum allowable reactor power

The magnitude of the risk $R_U(\theta, \tau)_{\text{norm}}=\gamma \cdot P^*$ will be called normalized because based on (4)–(7), it is the maximum permissible one in the event d_U. Thus, if $R_U(\theta, \tau)>R_U(\theta, \tau)_{\text{norm}}$, then continuation of the power unit operation in the existing mode is unacceptable. In this case, it is necessary to either stop the power unit or reduce the reactor power.

Let us find the maximum permissible power $V_U(\tau)$ of the reactor, at which the following condition is fulfilled

$$R_U(\theta, \tau) \le R_U(\theta, \tau)_{\text{norm}}. \tag{8}$$

Taking into account (3), inequality (8) gives

$$R_U(\theta,\tau) = \gamma \cdot \frac{V_U(\tau)}{W_0} \cdot p(d_U(\tau)) \cdot P(E_U(\tau)) \le \gamma \cdot P^*. \tag{9}$$

Since the event d_U has already occurred, then $p(d_U(\tau))$=1, and from (9) we obtain

$$\gamma \cdot \frac{V_U(\tau)}{W_0} \cdot P(E_U(\tau)) \leq \gamma \cdot P^* .$$

From which

$$V_U(\tau) \leq \frac{W_0 \cdot P^*}{P(E_U(\tau))} . \qquad (10)$$

Thus, the maximum permissible value to which the reactor power must be reduced is equal to

$$V_U(\tau)_{\text{perm}} = \frac{W_0 \cdot P^*}{P(E_U(\tau))} . \qquad (11)$$

At the same time, we note that in the case of $P(E_U(\tau))>P^*$, inequality (10) cannot be fulfilled, since $V_U(\tau)$ must always be less than the nominal reactor power W_0.

So, we have the following algorithm of actions in case of occurrence of event d_U. If $P(E_U(\tau))<P^*$, then it is possible to reduce the reactor power to the value (11), or, based on additional considerations, further reduce its power up to shutdown. In case $P(E_U(\tau))>P^*$, shutdown of the reactor is mandatory.

Note that a similar method of estimating the maximum permissible reactor power can also be used in case of forecasting the initiating event d_U. In this case, $p(d_U(\tau))<1$ and (9) gives

$$V_U(\tau)_{\text{perm}} = \frac{W_0 \cdot P^*}{p(d_U(\tau)) \cdot P(E_U(\tau))} . \qquad (12)$$

When using (12), as in the case of the occurrence of the event d_U, it is necessary to check the condition $V_U(\tau)_{\text{perm}}<W_0$, i.e. $p(d_U(\tau))\cdot P(E_U(\tau))<P^*$, and in case of its violation the only way out is to stop the reactor.

Example of determining the maximum allowable reactor power

As an example, let us consider the problem of reducing the power of a VVER-1000 reactor in the event of a failure to close one of the main safety valves of the pressurizer power-operated relief valve (PORV).

The nominal thermal power of the VVER-1000 reactor is 3000 MW. According to [6], the probability of failure of the PORV is $5\cdot10^{-3}$. Taking the highest probability limit of a design basis accident $P^*=10^{-4}$ [1], according to (11) we obtain

$$V_U(\tau)_{\text{perm}} = \frac{W_0 \cdot P^*}{P(E_U(\tau))} = \frac{3000\cdot10^{-4}}{5\cdot10^{-3}} = 60 \text{ MW},$$

i.e. in case of the PORV failure, the reactor power must be reduced to at least 60 MW.

However, if the power unit operator believes, based on the current situation at and around the plant, that the PORV failure may lead to a beyond design basis accident, then $P^*=10^{-7}$ and in this case, according to (11), $V_U(\tau)_{\text{perm}}$=0.06 MW, i.e. the reactor should be shut down.

Conclusions

The proposed accident risk assessment methodology allows to give a hint to the power unit operator when making a decision on adjusting the reactor power or its complete shutdown. Such a hint reduces the risk of making wrong decisions, i.e. reduces the influence of the human factor.

We also note that for many design-based accidents and various scenarios of their development, calculations according to formulas (11), (12) can be made in advance and the obtained results can be integrated as a database in the APCS of the power unit.

All these measures can be taken to increase the safety of NPP operation, especially under extreme conditions.

References

1. (2024). NP 306.2.245-2024 *Zahalni polozhennia bezpeky atomnykh stantsii* [General provisions on the safety of nuclear power plants] / State Nuclear Regulatory Inspectorate of Ukraine (in Ukrainian). https://zakon.rada.gov.ua/laws/show/z0598-24#Text.
2. Sevbo, A. Ye. & Taranovskiy, A. V. (2011). *Sostoyaniye problemy upravleniya riskami pri ekspluatatsii AES* [State of the art in risk management during NPP operation]. *Yadernaya i radiatsionnaya bezopasnost – Nuclear and Radiation Safety*, vol. 52, no. 4, pp. 49–55 (in Russian). https://doi.org/10.32918/nrs.2011.4(52).08.

3. Mukhopadhyay, S., Hastak, M., &Halligan, J. (2014). Compare and contrast major nuclear power plant disasters: Lessons learned from the past. In Rapp, R. R., Harland, W. (eds.), The Proceedings of the 10th International Conference of the International Institute for Infrastructure Resilience and Reconstruction (I3R2) (20–22 May 2014). West Lafayette, Indiana: Purdue University, pp. 163–169. https://doi.org/10.5703/1288284315360.
4. Yeliseyeva, M. A. & Malovik, K. N. (2014). *Sistematizatsiya metodov otsenivaniya riskov ekspluatatsii AES* [Systematization of methods for assessing NPP operational risks]. *Yadernaya i radiatsionnaya bezopasnost – Nuclear and Radiation Safety*, vol. 61, no. 1, pp. 21–25 (in Russian). https://doi.org/10.32918/nrs.2014.1(61).04.
5. Kalko, Ye. V., Dybach, A. M., Sevbo, A. Ye., & Kudla, Ye. P. (2012). Kontseptsiya operativnogo veroyatnostnogo analiza bezopasnosti [Concept of living probabilistic safety assessment]. Yadernaya i radiatsionnaya bezopasnost – Nuclear and Radiation Safety, vol. 55, no. 3, pp. 51–57 (in Russian). https://doi.org/10.32918/nrs.2012.3(55).11.
6. Stashevskiy, S. V. & Yarovoy, V. D. (2002). Ispolzovaniye veroyatnostnoy modeli energobloka no. 5 ZAES dlya otsenki effektivnosti zameny oborudovaniya AES [Using a probabilistic model of power unit no. 5 of Zaporizhzhya NPP to assess the effectiveness of replacing NPP equipment]. Proceedings of Sixth International Information Exchange Forum. Safety Analysis for Nuclear Power Plants of VVER and RBMK Types (April 8–12, 2002, Ukraine Kyiv) (in Russian). http://www.insc.gov.ua/forum6/doc/text/stashevsky.pdf.

Received 04 September 2025
Accepted 06 October 2025

Оперативний імовірнісний аналіз безпеки атомної електростанції, що працює в екстремальних умовах

А. О. Костіков, Л. І. Зевін

Інститут енергетичних машин і систем ім. А. М. Підгорного НАН України,
61046, Україна, м. Харків, вул. Комунальників, 2/10

Розглянуто проблему оперативного оцінювання ризику експлуатації атомної станції в екстремальних умовах, які можуть істотно вплинути на ядерну й радіаційну безпеку. На основі підходу, що ґрунтується на ймовірнісному аналізі безпеки, отримано методику для оцінювання ризику аварії, застосування якої дозволить персоналу станції при настанні події, що може істотно вплинути на безпеку експлуатації, швидко приймати рішення щодо необхідності зниження потужності реактора або зупинення енергоблока. Отримано формулу для обчислення максимально допустимої величини потужності реактора, за якої можна продовжувати експлуатацію станції в екстремальних умовах. Показано, що у разі подій, які становлять значний ризик і у змозі призвести до аварій, доцільно зупиняти блок, оскільки можуть бути порушені межі його безпечної експлуатації.

***Ключові слова**: атомна станція, ймовірнісний аналіз безпеки, максимально припустима величина потужності реактора, зупин реактора.*

Література

1. НП 306.2.245-2024 Загальні положення безпеки атомних станцій / Державна інспекція ядерного регулювання України. Київ, 2024. https://zakon.rada.gov.ua/laws/show/z0598-24#Text.
2. Севбо А. Е., Тарановский А. В. Состояние проблемы управления рисками при эксплуатации АЭС. *Ядерная и радиационная безопасность*. 2011. № 4 (52). С. 49–55. https://doi.org/10.32918/nrs.2011.4(52).08.
3. Mukhopadhyay S., Hastak M., Halligan J. Compare and contrast major nuclear power plant disasters: Lessons learned from the past. In Rapp R. R., Harland W. (eds.) The Proceedings of the 10th International Conference of the International Institute for Infrastructure Resilience and Reconstruction (I3R2) (20–22 May 2014). West Lafayette, Indiana: Purdue University, 2014. P. 163–169. https://doi.org/10.5703/1288284315360.
4. Елисеева М. А., Маловик К. Н. Систематизация методов оценивания рисков эксплуатации АЭС. *Ядерная и радиационная безопасность*. 2014. № 1 (61). С. 21–25. https://doi.org/10.32918/nrs.2014.1(61).04.
5. Калько Е. В., Дыбач А. М., Севбо А. Е., Кудла Е. П. Концепция оперативного вероятностного анализа безопасности. *Ядерная и радиационная безопасность*. 2012. № 3 (55). С. 51–57. https://doi.org/10.32918/nrs.2012.3(55).11.
6. Сташевский С. В., Яровой В. Д. Использование вероятностной модели энергоблока № 5 ЗАЭС для оценки эффективности замены оборудования АЭС. Материалы VI международного форума по обмену информацией «Анализ безопасности атомных электростанций с реакторами ВВЭР и РБМК», 8–12 апреля 2002, Украина, Киев. http://www.insc.gov.ua/forum6/doc/text/stashevsky.pdf.