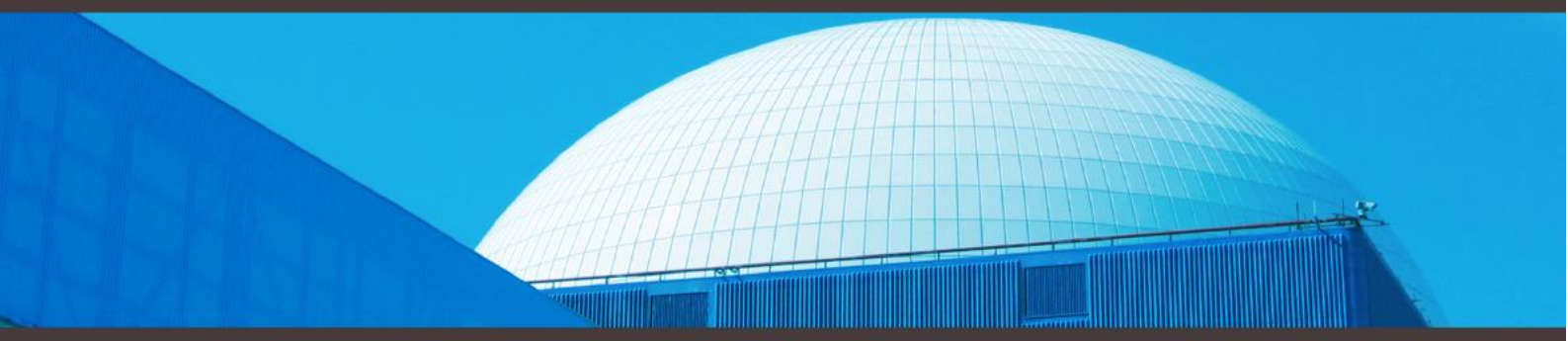
GIF/RSWG/2023/001

GEN IV International Forum
Expertise | Collaboration | Excellence

A RISK-INFORMED FRAMEWORK FOR SAFETY DESIGN OF GENERATION IV SYSTEMS

June 2023



DISCLAIMER

This report was prepared by the Risk and Safety Working Group of the Generation IV International Forum (GIF). Neither GIF nor any of its members, nor any GIF member‘s national government agency or employee thereof, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by GIF or its members, or any agency of a GIF member’s national government. The views and opinions of authors expressed therein do not necessarily state or reflect those of GIF or its members, or any agency of a GIF member’s national government.

Table of Contents

A RISK-INFORMED FRAMEWORK FOR SAFETY DESIGN of GENERATION-IV SYSTEMS

1. INTRODUCTION

Novel aspects of numerous advanced reactors would benefit from a systematic and technology-neutral approach for identification and categorization of event sequences to support their design and licensing. The risk-informed approach[1] offers an iterative process, complementary to the traditional deterministic approach, for a more comprehensive search of event sequences including their expected frequency and consequences to understand the risk. The approach can also support safety classification of plant equipment and defence-in-depth (DiD) assessment as an integral part of the process to ensure compliance with safety design criteria and establish links between *required safety functions* and design requirements.

This position paper is intended to provide an example of framework for such a risk-informed approach in application to Generation-IV systems, recognizing that different approaches are also possible to risk-inform a design. The framework borrows from previously proposed risk-informed performance-based guidance for licensing basis development by the Nuclear Energy Institute.[1] While Reference [1] was developed based on the U.S. regulatory codes and standards, our position paper includes broader considerations to generalize the approach for other regulatory frameworks mainly based on International Atomic Energy Agency (IAEA) safety standards. It discusses how a risk-informed design process can combine both deterministic and probabilistic insights into the decision-making in a complementary way to inform the safety design and demonstrate alignment with DiD principles.

In particular, the approach aims to:

- establish generic event sequence categories to be considered in design, and integrate the deterministic input and risk insights to identify and classify the event sequences in each category,
- define the main elements of a generic frequency-consequence target to evaluate the event-sequences against a generic set of regulatory requirements and risk goals,
- establish a process to classify the plant equipment based on their risk-significance and the role in plant safety (prevention or mitigation functions within each event sequence),
- support deterministic phenomenological analysis of the key event sequences considered in design consistent with the safety classification of the responding plant equipment,
- assess the alignment of event sequence categories considered in design with the DiD levels, and
- establish the process for treatment of low-frequency event sequences as residual risk, including the consideration of high-consequence cliff-edge effects to ensure that the possibility of conditions with potential for large or early releases are ‘practically eliminated’.

[1] Unlike the risk-based approach that relies solely on risk assessments, in the risk-informed approach, the technical insights from traditional deterministic approach based on past performance, expert judgment, and findings of engineering analyses are considered as an input in combination with the risk insights when assessing design safety.

2. FOUNDATIONAL CONCEPTS

To achieve consensus among the members of GIF Risk and Safety Working Group (RSWG), as well as the CNRA Working Group on Safety of Advanced Reactors (WGSAR) members who reviewed the proposed framework and provided valuable feedback, the internationally recognized IAEA terminology and corresponding definitions are preferred throughout this position paper. The sentences quoted from the IAEA safety glossary[1] and the key concepts quoted from the IAEA safety standards and other references are included in *italic* letters.

2.1 Defence-in-Depth

Defence-in-Depth is a concept that refers to "*a hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.*"[2]

DiD is implemented primarily through several consecutive and independent levels of protection to compensate for component failures and human induced events as shown in Table 1. When properly implemented, DiD ensures that no single technical, human or organizational failure could result in harmful effects, and the combination of failures that could give rise to significant harmful effects are of very low probability.

Table 1. IAEA's Defence-in-Depth (DiD) levels and their purpose.

DiD level	1. Purpose
1	Prevent deviations from normal operation and the failure of *items important to safety*.
2	Detect and control deviations from normal operation in order to prevent anticipated operational occurrences from escalating to accident conditions.
3	Prevent damage to the reactor core and releases of radioactive material requiring off-site protective actions, and to return the plant to a safe state by means of inherent and/or engineered *safety systems* and procedures.
4	Prevent the progress, and to mitigate the consequences, of accidents that result from failure of the third level of defence by preventing accident sequences that could lead to large or early releases of radioactive material.
5	Mitigate radiological consequences of radioactive material release that could potentially result from an accident condition.

NOTE: This IAEA structure introduces the "cascading failures" concept to capture the accidents progressing to successive levels. The risk-informed approach retains this consideration, but it could also potentially identify "non-cascading" event sequences (such as a DBA initiator) that might otherwise be missed.

2.2 Plant equipment classification

The terminology for the safety classification of the plant equipment adopted in this position paper is shown in Figure 1. Since terminology differs significantly in each country, the plant

equipment classification and corresponding definitions are based on IAEA safety standards and glossary [2] to establish an internationally recognized common terminology.

An *item important to safety* is a plant equipment whose malfunction or failure could lead to radiation exposure of the site personnel or public. The *items important to safety* include:

- The *safety related item,* defined as "*a system important to safety that is not part of a safety system*"[2] primarily intended to prevent an anticipated operational occurrence leading to an accident condition.
- The *safety system*, defined as "*a system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents*".[2]
- The *safety features* that inherently have, or designed to perform, a safety function for design extension conditions to mitigate the consequences of malfunction or failure of *safety systems*.

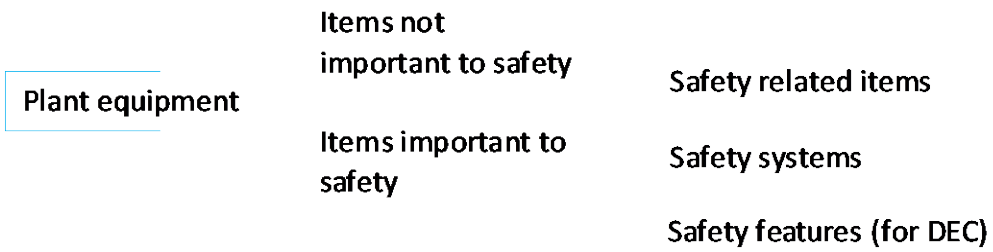


Figure 1. Safety classification for plant equipment (a structure, system, or component).

2.3 Initiating events and event sequences

An event sequence is comprised of an initiating event, a sequence of involved plant equipment and/or operator response, and a stable end-state that characterizes the impact of the sequence on the plant or the environment (e.g., prevention of radioactivity release or release in one of the consequence categories). The initiating event may be associated with an internal event such as an equipment failure or human error, an internal plant hazard such as a fire or flood, or an external event such as an earthquake or tsunami. The event sequences resulting from an initiating event then depend on the plant design, operator response, and additional failure assumptions for the involved plant equipment in these sequences. Therefore, depending on the plant design and its response, the same initiating event could lead to different categories of event sequences based on the frequency of occurrence of each event sequence.

2.4 Event sequence categories considered in safety approach

The plant states considered in design and corresponding definitions are summarized in Table 2. The categories and definitions in Table 2 are intended to establish a common terminology based on IAEA safety glossary [2] while recognizing that they will need an alignment with the regulatory requirements in each member state. The phrase "accident conditions" in the IAEA terminology equates to "event sequences categorized as Design Basis Accident (DBA) or Design Extension Condition (DEC)" within the context of this position paper. The Anticipated Operational Occurrences (AOOs) that are defined as a deviation from Normal Operation (NO) may also involve an event sequence resulting from this deviation.

Table 2. Plant states considered in design.

Category	Definition	Responding Plant Equipment*
Normal Operation (NO)	Operation within specified limits and conditions, including startup, power operation, shut down, maintenance, testing and refueling.	NO usually does not rely on the *required safety function* of any plant equipment classified as *items important to safety*.
Anticipated Operational Occurrence (AOO)	*A deviation of an operational process from normal operation expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.*[2] AOO category refers to the event sequences resulting from the "deviation" defined above.	Once the safety-classification of the plant equipment is completed, only the *safety related items* are considered to prevent AOOs from leading to accident conditions. The *safety systems* are usually excluded from responding to an AOO except for fulfillment of the confinement function.
Design Basis Accident (DBA)	*A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.*[2] DBAs are infrequent event sequences not expected to occur in the life of a nuclear power plant and are less likely than AOOs. The continuous capability to respond to DBAs is the basis for the design, construction, and operation of the plant equipment.	Once the safety-classification of the plant equipment is completed, only the *safety systems* are considered to provide an acceptable plant response and outcome for DBAs. Therefore, DBAs are used to set performance and safety requirements for the design of *safety systems*.
Design Extension Condition (DEC)	*Postulated accident conditions not considered for design basis accidents, but considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits.*[2] DEC are very rare event sequences that are not expected to occur in the life of a nuclear reactor fleet, are typically less likely than DBAs (with some potential overlap with DBAs). Despite their very low frequency of occurrence, they are still considered in the design.	Once the safety-classification of the plant equipment is completed, independent *DEC safety features* are considered to prevent off-site releases or mitigate and limit the consequences to within the regulatory dose limits assuming *safety systems* that perform similar functions for DBAs may not ALL be available or fully functional (DEC mitigation may rely on availability of some *safety systems* if their failure is not part of the event sequence under consideration).

* Safety barrier function is not considered in Table 2.

The NO, AOOs and DBAs are collectively considered as the *design basis conditions* for which the plant is designed according to the established design criteria and evaluated via conservative methodology.[2] The DECs are specific set of accident sequences that go beyond the *design basis conditions*, selected on deterministic and probabilistic basis, including complex multiple failure sequences and *severe plant conditions*.[2] Although DECs are evaluated in accordance

[2] The term "*severe plant condition*" is notionally meant to imply the DEC-B category of events that include "severe accidents with core melt", when applicable. Since a core melt is not applicable to some Generation-IV designs, the term "*severe plant conditions*" is used consistent with the terminology adopted in Reference 2.

with the best estimate methodology, the *required safety function* of the responding *plant equipment* and *safety features* must be met with sufficient margins to compensate for the uncertainties and avoid cliff edge effects. Appropriate design rules and the applicable criteria are also established for DECs, in addition and complementary to those for DBAs.[3]

The event sequences with sufficiently low frequency of occurrence are not considered in further analysis due to implementation of DiD principles. The practically eliminated situations (PES) that could potentially lead to large off-site radioactive releases, or with kinetics that would not allow timely and reasonable implementation of necessary measures to protect populations (early releases), are required to be ruled out from the design through a robust demonstration that shows they are either physically impossible or extremely unlikely with a high degree of confidence.[3] Such excluded "situations" would still require a robust demonstration of the prevention and mitigation measures with high degree of confidence, backed with surveillance, inspection, and periodic testing procedures.

2.5 Frequency-Consequence Target

This risk-informed approach uses a set of frequency-consequence criteria to represent the risk and establish a correlation between the permissible dose limits and frequency targets when evaluating the event sequences. Such a generic correlation, referred to as "*frequency-consequence target*" in this position paper, is shown in Figure 2 as a simplistic example. The frequency and dose limits for the AOO, DBA, and DEC event sequence categories vary from country-to-country and some overlap may exist between DBA and DEC categories. Nevertheless, the overall structure of the *frequency-consequence target* concept will likely be generally applicable for a systematic representation of high-level frequency and dose requirements and can be revised to accommodate these variations without an impact on the other concepts introduced in this position paper.

In the context of Figure 2, the risk is defined as "the product of the frequency and consequence", and the acceptable risk is delineated by the red "risk-target" against which the risk and safety significance of, and relative safety margins for, the individual event sequences are evaluated. Although shape of the risk-target will vary and may look more like a staircase, its shape is generally optimized to balance the risk profile across the entire frequency and consequence spectra and minimize the integral risk for the whole plant design consistent with the national regulatory limits.

The *frequency-consequence target* provides a tool to differentiate between increasing and decreasing risk, and to compare the risk with the applicable regulatory requirements related to public safety. The consideration of the "risk-target" allows addressing the full set of possible plant conditions categorized as a function of their estimated frequency of occurrence. The idea is to achieve balanced and optimal risk reduction by assuring insignificant consequences for the frequent events, and extremely low frequencies for event sequences with high potential consequences and *severe plant conditions*.

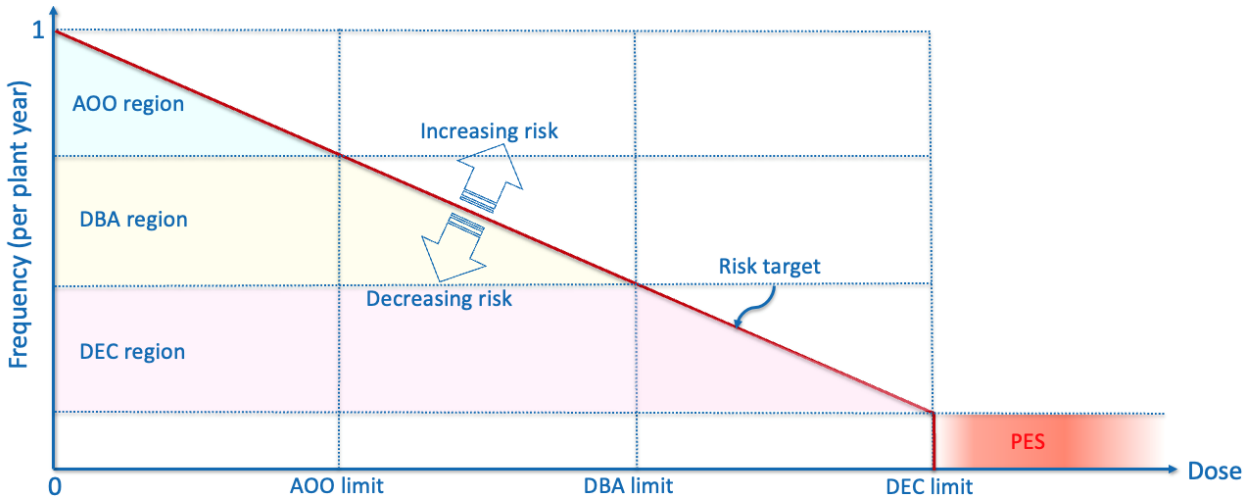


Figure 2. Frequency-Consequence Target.

Once the system safety architecture is defined, the designer must prove that, for all the design basis and design extension conditions, the system response allows the corresponding risk to be kept within the tolerable domain—below the risk-target with margin. Risk-significance of the involved plant equipment is also evaluated so that their safety classification is consistent with the role they play to keep the risk below the risk-target for all event sequences, again with margin. The vertical portion of the risk-target is intended to imply that there should be no acceptable frequency for large releases (the domain beyond the vertical portion of the risk-target indicate large releases that are to be practically eliminated).

3. ELEMENTS OF RISK-INFORMED DESIGN PROCESS

The risk-informed approach is a systematic process repeated in different design stages to establish the safety basis and demonstrate that the identified event sequences adequately cover the full range of hazards and conditions a design can be exposed to. The approach is technology-neutral and can also ensure that the plant equipment that perform a *required safety function*[3] are adequately capable, reliable, redundant, and diverse across the DiD layers. The major elements of the risk informed process to identify and categorize the event sequences and support safety classification of the plant equipment are summarized in Figure 3, and each item in the figure is further discussed below.

[3] A function required to maintain the risk from one or more event sequences inside the F-C Target while also meeting the *cumulative risk targets* such as the annual dose limit and/or the risk for early/latent fatalities.

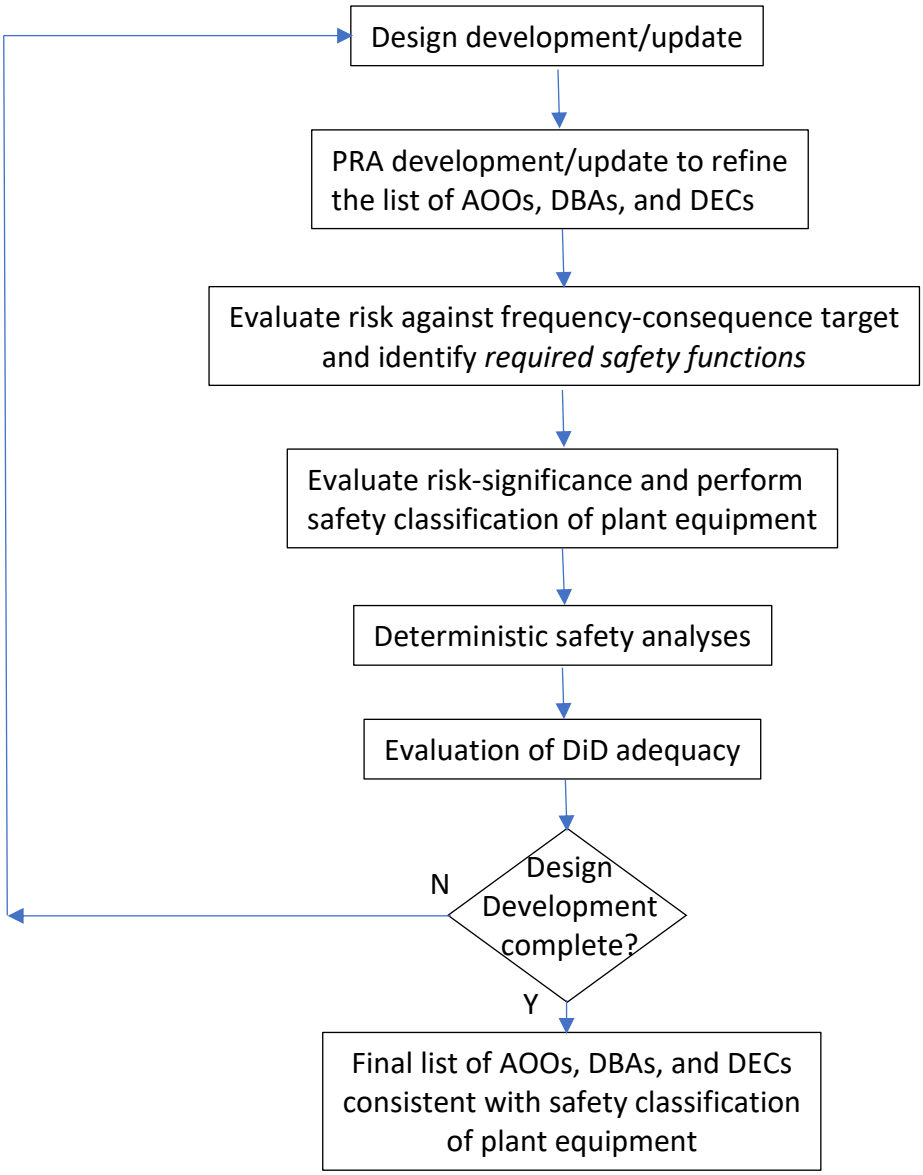


Figure 3. Process for selection of AOOs, DBAs and DECs.

The process is repeated for each design phase until the list of AOO, DBA and DEC event sequences becomes stable. Because the categorization of event sequences requires the proper classification of safety- and risk-significant structures, systems and components, the process also facilitates the selection of *safety related items*, *safety systems*, and *safety features* that are key for design completeness in compliance with DiD principles.

3.1 Design development/update

A plant design is performed in phases, typically starting with the conceptual design and progressing through the preliminary and final design stages. The initial design development process may include:

- Definition/refinement of the safety approach through the use of Qualitative Safety-features Review (QSR)[3] for identification and fine-tuning of design features to meet the safety design criteria,

- Development of Phenomena Identification and Ranking Table (PIRT) [3] to evaluate and build sufficient knowledgebase for the deterministic safety analyses and probabilistic risk assessments,
- Identifying the specific provisions to fulfil the *required safety functions* at each DiD level using tools like Objective Provision Tree (OPT) [3], and
- Assessment of the effectiveness of the Lines of Protection (LOP) [3] for the set of safety functions, challenges, mechanisms, and provisions in a consistent manner for each DiD level through initial evaluation of their capability, reliability, diversity, and the conditions of their mutual independence (and interdependence, to avoid common-cause failures).

QSR, PIRT, OPT and LOP all provide opportunities for early identification of safety vulnerabilities and their qualitative contributions to risk during initial stages of the concept development so that new design improvements can be identified, developed, and implemented to achieve safety-by-design principles. These tools can contribute to initial understanding of risk factors, safety margins, effectiveness of safety-related design measures, and sources of uncertainties. This step also facilitates first identification of the initiating events and event sequences to be considered in design, as well as the sequences to be excluded or practically eliminated.

The initial set of initiating events and event sequences are identified mainly deterministically based on expert judgment and insights from technology-specific safety design criteria and guidelines [4], but the list may also be supported by qualitative risk insights based on prior experience from operation of similar reactors. Although the first list of initiating events and event sequences will likely be incomplete, the list is gradually revised and expanded throughout the design iterations including the risk-informed input as discussed in following steps.

3.2 PRA development/update to refine the list of AOOs, DBAs, and DECs

The Probabilistic Risk Assessment (PRA), also known as Probabilistic Safety Assessment (PSA), provides a structured means to answer three basic questions: What can go wrong, how likely is it to occur, and what are the consequences? The PRA is traditionally used for Generation-II and -III reactors to evaluate core damage frequency and assess the risk from bounding accident sequences. As part of the risk-informed approach, PRA involves the analysis of all event sequences for consequence assessments in the entire frequency spectrum to support identification and implementation of the risk management strategies by providing risk insights to supplement the deterministic design process.

The PRA models can be developed, and the risk assessments may be performed, at any design stage. However, the benefits of incorporating the risk insights into the design favor its early introduction to achieve safety-by-design principles. The scope and level of detail of a PRA model enhance as the design matures, new reliability data from component testing becomes available, and the site is selected. The PRA model is often updated to reflect changes in the design and system configuration and the results, in return, influence the design process by contributing to key decisions for new safety measures by studying the risk space. PRA also facilitates a systematic understanding of the uncertainties related to risk. Uncertainties arise from several causes and are typically accommodated in a design through additional safety margins. PRA can help identify the sources of these uncertainties to achieve an optimized and balanced design by considering their impact on reliability.

Prior to its introduction, the PRA requires a sound understanding of the potential failure modes, the plant's response to such failures, and the protective strategies that can be incorporated into the design. The PRA systematically analyzes event sequences and assesses the frequency of

each event sequence including internal events, human errors, and external hazards. The modeled event sequences also include the contributions from common-cause failures. They may also incorporate multi-unit events where two or more reactors on the same site may have some interaction scenarios. The PRA provides important input to the formulation of design requirements and performance targets for the plant equipment in terms of their reliability to prevent these events, and in terms of their capability (capacity) to mitigate the consequences.

The event sequences obtained from the PRA are used as additional input to confirm or revise the initial deterministically developed list of event sequences considered in the design. The event sequences modeled and evaluated in the PRA are grouped into event sequence families, each having a similar initiating event, dynamic plant response, and an end state potentially with dose consequences if a radiological release is anticipated. Bounding event sequences in each of these families (with most severe consequences) are assigned to an event sequence category (AOO, DBA, or DEC) based on event sequence frequency of occurrence per plant-year. Event sequences with frequencies slightly beyond the cut-off threshold are still retained in the PRA model to confirm that there are no cliff-edge effects as part of the risk-informed evaluation of DiD (as discussed in section 3.6). In addition to this input from PRA, the expert judgment and utilization of relevant experience continue to be relied on to ensure that event sequence selection and categorization is comprehensive and does not override deterministic insights.

3.3 Evaluate risk against frequency-consequence target and identify required safety functions

The results of the PRA for all event sequences are weighed against the *frequency-consequence target* (introduced in Figure 2 as a simplistic example) to evaluate risk, establish the dominant risk domain, and focus the attention on the risk-significant event sequences and possible means to address their consequences. The risk is evaluated against the *frequency-consequence target* based on the mean estimates, but the PRA process should also consider the uncertainties in both the frequency and dose estimates using quantitative uncertainty and sensitivity analyses.

The primary purpose of this step is to evaluate the risk-significance of each event sequence based on the response of the involved plant equipment. Another objective is to identify design features and plant equipment that are responsible for preventing/mitigating radiological releases and meeting the *cumulative risk targets*[4] to manage the integrated risks from consideration of all event sequences. This information is then used to evaluate the risk significance of plant equipment in support of their safety classification as discussed in the next step.

The full set of AOOs, DBAs and DECs are examined to identify the *required safety functions* and ensure that the specified offsite dose requirements can be conservatively met for each event sequence category considered in design. The *required safety function* for AOOs is to prevent them from progressing to accident conditions, posing challenges to the *safety systems*, and exceeding the associated dose limits. The *required safety functions* for DBAs and DECs are both to prevent and mitigate their risk to within their respective dose limits. For any high-consequence event, the preventive safety functions are also responsible for reducing the event sequence frequency by exhibiting sufficient reliability performance.

The risk-informed approach highlights and informs the necessary considerations of both prevention and mitigation functions. The *required safety function* identification is illustrated conceptually in Figure 4 with the horizontal arrow for the mitigation function and vertical

[4] Typical *cumulative risk targets* include an annual dose limit and/or the risk for early/latent fatalities.

arrow for the prevention function. Although most event sequences are not expected to result in a release of radioactive materials (no dose consequences), they are still evaluated to facilitate identification of plant capabilities needed to assure prevention of such releases, and to support safety classification of the responding plant equipment as discussed below.

3.4 Evaluate risk significance and perform safety classification of plant equipment

The purpose of this step is to identify design features and plant equipment that are responsible for keeping the event sequences well within the *frequency-consequence target* including those for preventing or mitigating above-limit releases. In addition to the predicted risk for each event sequence, the integrated risk for all event sequences is used to define the safety- and risk-significance of the plant equipment (including the barriers) and intrinsic design characteristics.

For each *required safety function* identified in previous step, one or more plant equipment and intrinsic design characteristics (among those found to be available for the spectrum of AOOs, DBAs and DECs) are identified as safety-significant. The requirements for these safety-significant plant equipment include the preventive capabilities to meet the reliability targets (to reduce the failure frequency) and the capabilities to facilitate their mitigation functions (to reduce dose consequences). A safety-significant plant equipment is broadly defined as an *item important to safety* in a way that it performs a general safety function necessary to achieve adequate protection.

In comparison, a plant equipment is considered risk-significant if its safety function is essential to keep the risk from one or more event sequences within the "risk limit" (under the red *frequency-consequence target*) based on predicted mean frequencies and consequences. In other words, if the subject plant equipment malfunctions, the risk would be unacceptably high, challenging the dose limits or event sequence categorization. A plant equipment is also considered risk-significant if the integrated risk for all event sequences with the failed plant equipment exceeds the *cumulative risk targets*. The risk-significant plant equipment that may perform a *required safety function* for prevention or mitigation is depicted in Figure 4.

The risk-significant plant equipment typically includes some key *safety systems* for DBAs and *safety features* for DECs. While the safety-significant plant equipment generally enhances the safety of a design (to eliminate an acceptable but dominant risk, for example), the *required safety function* of a risk-significant plant equipment is essential to achieve the overall risk-informed design of the plant (without it, the risk limits would not have been met). The plant equipment safety classification is performed based on evaluation of their performance to fulfill the *required safety functions* as illustrated in Figure 5.

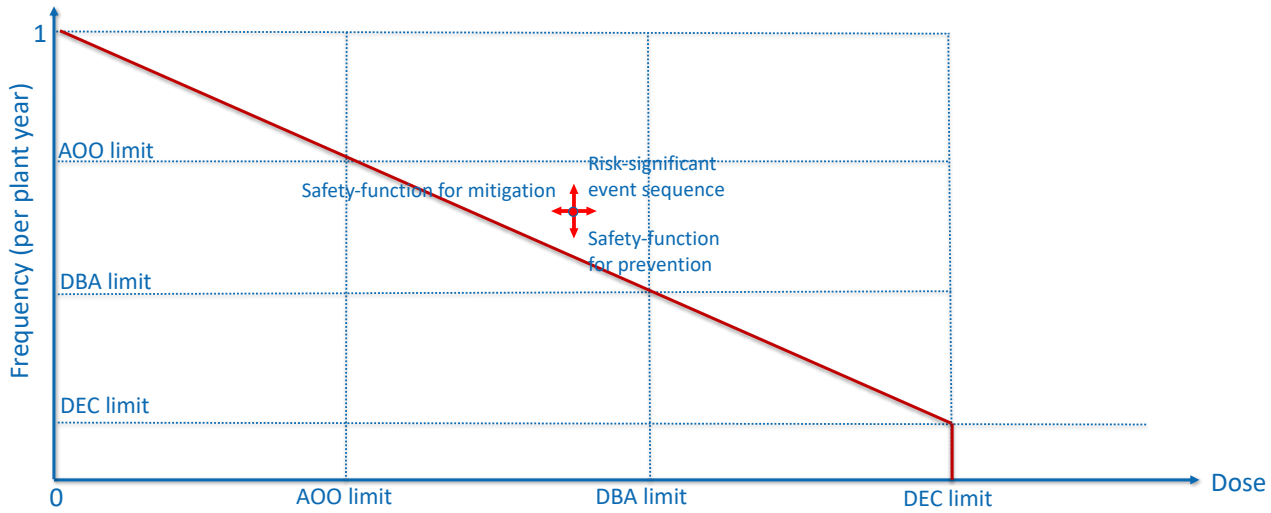


Figure 4. Identification of prevention and mitigation functions illustrated on frequency-consequence target for an above-target event sequence.

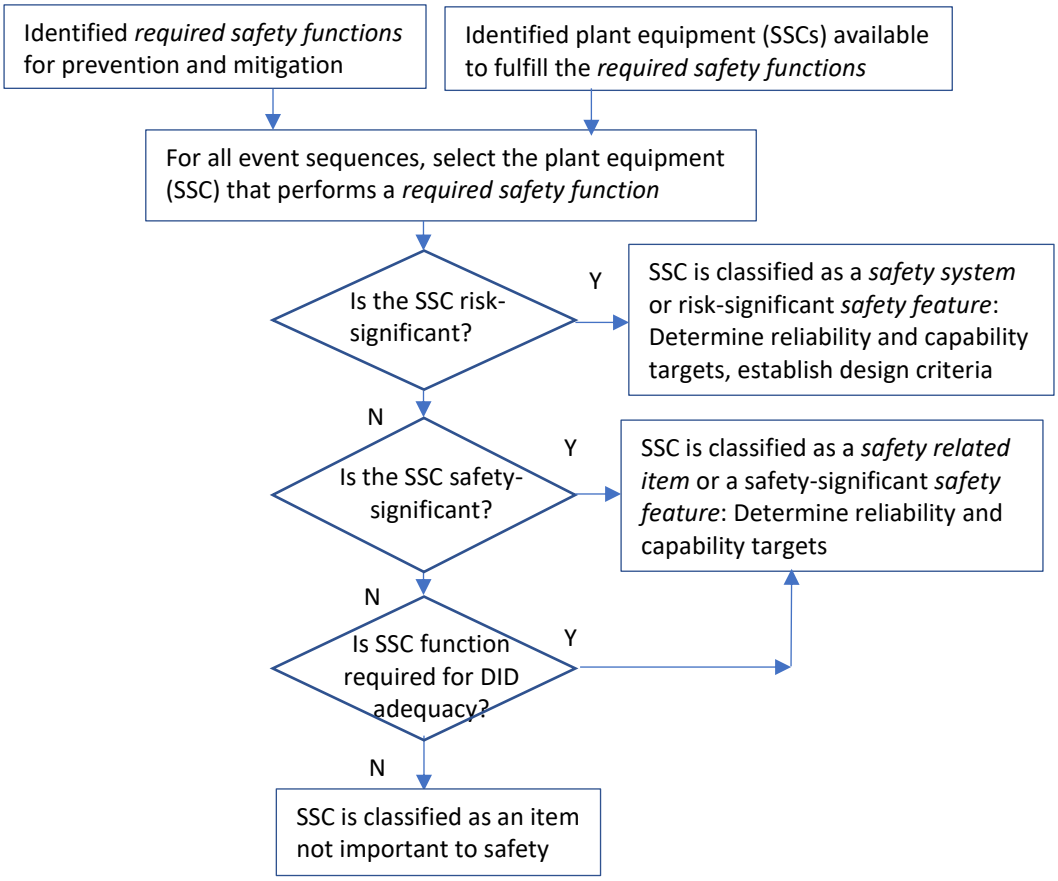


Figure 5. The process for safety classification of, and establishment of design requirements for, the plant equipment (SSC).

The plant equipment safety classification steps are as further described below:

- Each risk-significant event sequence (those that land above the frequency-consequence target and, unless prevented or mitigated, pose an unacceptable risk) is examined to

determine which plant equipment are available to perform the risk-significant *required safety functions*. Then, one or more of available *plant equipment* and *safety features* are selected to perform each safety function that covers all these risk-significant DBA and DEC event sequences.

- The minimum set of specific plant equipment that can be solely relied on during DBAs are classified as *safety systems*.
- The remaining plant equipment are further evaluated to determine if their safety function is necessary to keep the risk from one or more event sequences within the risk limit (the frequency-consequence target) or if they make significant contributions to maintain the *cumulative risk targets*.
    - If a plant equipment is classified as risk-significant but it is not a *safety system*, then it is classified as a risk-significant *safety feature* (an item or process that is designed to perform a safety function, or inherently has that safety function) intended for reliance in DECs.
    - If a plant equipment is not considered risk-significant but still performs a general safety function necessary to maintain or enhance the safety and further reduce risk (for example, to avoid the dominant risk or address related uncertainties in the event sequence), it is considered a safety-significant plant equipment and classified as a *safety related item*.
- The last step in the process is to confirm if the subject plant equipment plays a role in assessment of DiD adequacy. This step is to ensure that the *plant equipment* and *safety features* fulfill the required safety functions independently at each layer of defence and to address uncertainties in their performance. If a plant equipment plays a role in ensuring DiD adequacy, then it is considered safety-significant. If not, it is considered as an *item not important to safety*.

For each classified plant equipment, the reliability and capability requirements are established, and corresponding design requirements are identified to ensure their maintained capability and reliability throughout the plant lifetime. When evaluating a plant equipment, we also consider its role in all event sequences to establish the integrated risk from their failure against the cumulative risk targets such as the annual dose limit.

To repeat, a risk-significant plant equipment reduces the frequency or consequence of a risk-significant event-sequence so that the associated risk falls within limits. Safety-significant plant equipment further reduces the frequency or consequence of an event-sequence mainly to address the dominant risk (when the risk is below the risk-target, but uncomfortably close to it) or address uncertainties in frequency and consequence predictions. Broadly speaking, all safety-significant plant equipment are the "items important to safety." In comparison, a risk-informed plant equipment is a key "*safety system*" that is relied on during DBAs, or a key "*safety feature"* for DEC to keep the risk within limits.

3.5 Deterministic safety analyses

The step for deterministic safety analyses involves the traditional deterministic and phenomenological analyses for design verification to confirm that the plant can withstand the full range of conditions and events considered in the design. They involve thermal-hydraulic analyses, computational fluid dynamics (CFD) analyses, reactor physics analyses, accident transient numerical simulations, models for fuels and materials behavior, and structural analyses to name a few. The deterministic safety analyses also aim to establish the effectiveness of lines of defence and their degree of independence, and to confirm the design basis for *items important to safety*.

As discussed in page 9, the large number of event sequences resulting from the PRA are grouped into "families" and categorized in one of the event sequence categories shown in Table 2. The bounding event sequences in these families in AOO, DBA and DEC categories are evaluated depending on their realistically or conservatively estimated expected frequency of occurrence and potential consequences, each category with a unique set of acceptance criteria and analysis methodology consistent with the associated regulatory requirements.

- For each AOO family, an event sequence is defined assuming that the *required safety functions* are performed mainly by the plant equipment that are classified as *safety related items*. These AOOs are then studied typically using deterministic phenomenological analyses.
- For each DBA family, a bounding deterministic event sequence is defined assuming that the *required safety functions* are performed exclusively by the plant equipment that are classified as *safety systems*. All other plant equipment that may perform these same or similar functions are assumed to be generally unavailable for DBA analysis. These DBAs are then used in the design basis analysis of the license application for supporting the conservative deterministic safety analyses.
- Similarly, for each DEC family, a bounding event sequence is defined assuming that the *required safety functions* are performed by specific *safety features* for DEC to prevent off-site releases or mitigate and limit the consequences to within the regulatory dose limits. For DECs, some *safety systems* that perform the same or similar functions for DBAs may not be available or fully functional while others may be available if their failure is not part of the event sequence under consideration. The DECs are considered in the deterministic safety analyses usually in accordance with the best-estimate methodology, although BEPU approach is also considered in some countries to add additional robustness to the plant design.

3.6 Evaluation of defence-in-depth adequacy

This step involves confirming that the *frequency-consequence target* and *cumulative risk targets* for all event sequences are met in all DiD levels factoring in the uncertainties. Overall guidelines for the first four levels of DiD include reliance on at least two (ideally three) redundant and diverse means for each *required safety function* so that no single design or operational feature, no matter how robust or reliable, is exclusively relied on to achieve the overall design goals. The process for evaluation of DiD adequacy is outlined in Table 3.

Table 3. Process for evaluation of Defence-in-Depth adequacy

DiD Level	Guidelines to Achieve the Design Goals
1	Selection of appropriate design codes and materials, quality control of the component manufacturing and plant construction, and the processes/procedures for in-service inspection, maintenance and testing. Design options that reduce the potential for internal events also contribute to prevention of abnormal operations at Level 1.
2	Maintaining frequency of all AOO sequences to be within a specified limit per plant-year and well-below the allowed off-site dose consequences, also factoring in the uncertainties, while minimizing the challenges to the designated *safety systems*. This necessitates the provision of specific *safety related items* in the design and the confirmation of their effectiveness through deterministic safety analyses and probabilistic risk assessments.
3	Maintaining frequency of all DBA sequences to be within a specified limit per plant-year and well-below the allowed off-site dose consequences, also factoring in the uncertainties, while maintaining the effectiveness of *safety systems* that are relied on to return the plant to a safe end state, to avoid damage to the reactor core, and to prevent radioactive releases requiring off-site protective actions.
4	Maintaining individual risks from all event sequences within a specified limit per plant-year and the allowed regulatory dose limits with sufficient margin by mitigating the consequences of accidents that result from failure of the third level of defence in depth. This can also be achieved by preventing the progression of such accidents into a *severe plant condition*. The event sequences leading to an unacceptably early or large radioactive release are required to be 'practically eliminated' by implementing design provisions.

DiD is deemed to be adequate when:

- DiD guidelines to achieve the design goals listed in Table 3 are satisfied,
- risk margins against the *frequency-consequence target* are sufficient and *cumulative risk targets* are met,
- the role of plant equipment in prevention and mitigation at each layer of defence is understood, and prevention-mitigation balance is achieved without excessive reliance on one vs. the other (so that the plant safety does not hinge mostly on mitigation or preventive measures),
- independence of design features at each layer of defence is sufficient (so that the same *plant equipment* or *safety feature* is not primarily responsible for the plant safety in multiple DiD layers), and
- design margins in plant capabilities are adequate to address uncertainties identified in the PRA as well as the deterministic and phenomenological analyses.

Programmatic elements complement this process to address the uncertainties by providing means to incorporate additional safety attributes while designing, manufacturing, constructing, operating, maintaining, testing, and inspecting the plant, the specific plant equipment, and the associated processes for reasonable assurance that the predicted performance can be achieved throughout the lifetime of the entire facility.

Outcome of this step may include possible changes to the design to enhance the plant capabilities (including potential changes in safety classification of the plant equipment), formulation of conservative assumptions for the deterministic safety analysis, and input to defining and enhancing programmatic elements for manufacturing, construction, operation and maintenance, testing and inspection. The risk-informed evaluation of DiD adequacy is

considered complete when no new risk-significant vulnerabilities requiring additional compensatory actions are identified.

3.7 Decision on completion of design development

A decision is made if additional design development is warranted[5], either to proceed to the next logical design stage or to incorporate feedback from the event sequence evaluation that design, operational, or programmatic improvements should be considered. Such design improvements could be motivated by a desire to increase margins against the *frequency-consequence target*, reduce uncertainties in the event sequence frequencies or consequences, limit the need for restrictions on siting or emergency planning, or enhance the plant equipment reliability and capability against the established performance requirements and DiD criteria in Table 3. When the list of initiating events and associated event sequences are finalized, it will likely lead to a more robust design with more adaptive defence measures based on safety-by-design principles than what could be achieved via deterministic considerations alone.

4. SUMMARY

Further achievement of international cooperation in research and development for the next generation of nuclear energy systems, such as the six novel Generation-IV systems, requires good analytical support in the process of their design and licensing. One such analytical support is the technology-neutral risk-informed approach for systematic search and categorization of event sequences including their probability and consequences to understand the risks.

This position paper introduces foundational concepts and main elements of a risk-informed design process that combines both deterministic and probabilistic insights into the decision-making in a complementary way to inform the safety design and demonstrate alignment with defence-in-depth principles. The approach aims to

- establish the event sequence categories considered in design, and integrate the deterministic input and risk insights to identify and classify the event sequences in each category,
- define the main elements of a generic frequency-consequence target to evaluate the event-sequences against the associated regulatory requirements,
- establish a process to classify the plant equipment based on their risk-significance and the role in plant safety (prevention or mitigation functions within each event sequence),
- support deterministic phenomenological analysis of the key event sequences considered in design consistent with the safety classification of the responding plant equipment, and
- assess the alignment of event sequence categories considered in design with the defence-in-depth levels.

The proposed framework borrows from the risk-informed performance-based technology inclusive guidance proposed by the Nuclear Energy Institute in the U.S.[1] but intends to broaden its applicability by generalizing it for other regulatory frameworks mainly based on IAEA safety standards. The proposed framework is not a fully implementable process yet as additional layers are needed. Development of such a full-blown process will undoubtedly take

[5] Such a conclusion can be reached through an integrated decision-making process by a panel consisting of staff from across the different project elements (design and safety teams, etc.) who review both the probabilistic and deterministic results to determine if additional improvements are justified.

far more significant effort over many years requiring very substantial resources beyond the means of the GIF RSWG.

REFERENCES

[1] Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development, NEI Technical Report, NEI-18-04, August 2019.

[2] IAEA Safety Glossary (Terminology Used in Nuclear Safety and Radiation Protection), 2018 Edition, http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf , INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna (2019).

[3] "Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems," Revision 2, The Risk and Safety Working Group of the Generation IV International Forum (GIF), September 2020.

[4] Task Force on Safety Design Criteria, Generation IV International Forum (GIF), https://www.gen-4.org/gif/jcms/c_93020/safety-design-criteria.

A report produced by

GEN IV International Forum

Expertise | Collaboration | Excellence

www.gen-4.org

RSWG

Risk and Safety Working Group