25 YEAR ANNIVERSARY
GEN IV INTERNATIONAL FORUM
Expertise | Collaboration | Excellence

A risk-informed framework for Safety Design of Generation-IV Systems



November 2026

GIF/RSWG/2026/001

(This page has been intentionally left blank)

DISCLAIMER

This report was prepared by the Risk and Safety Working Group. 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.

Cover page design: Renodesign

Cover page photo: © iStock.com/Ryzhi

(This page has been intentionally left blank)

Abstract

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 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 defense-in-depth assessment as an integral part of the process to ensure compliance with safety design criteria and establish links between the 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 but includes broader considerations to generalize the approach for other safety frameworks mainly based on the International Atomic Energy Agency 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 defense-in-depth principles.

List of Authors

Members of the Risk and Safety Working Group (RSWG)

Tanju Sofu	Member	Argonne National Laboratory (ANL), USA
James Kinsey	Former Member	Idaho National Laboratory (formerly) (INL), USA
David Hummel	Co-Chair	Canadian Nuclear Laboratories (CNL), Canada
Luca Ammirabile	Member	European Commission Joint Research Centre (EC JRC)
Paul Gauthé	Former Member	French Alternative Energies and Atomic Energy Commission (CEA), France
Etienne Courtin	Member	Framatome, France

Acknowledgements

Generation IV International Forum gratefully acknowledges the contributions of Mr. Vincenzo Tiberi of the IAEA for his careful review of this report. His thoughtful comments, technical insights, and constructive recommendations were invaluable and led to substantial revisions that significantly strengthened the clarity, accuracy, and overall quality of the final document. While the responsibility for the content ultimately rests with the authors, this report has benefited greatly from the time and expertise generously provided by his reviews.

Table of Contents

Abstract i

List of Authors ii

Acknowledgements ii

Table of Contents iii

List of Figures iv

List of Tables iv

List of Acronyms v

1. Introduction 1

2. FOUNDATIONAL CONCEPTS 1
2.1. Defense-in-Depth 2
2.2. Plant equipment classification 2
2.3. Initiating events and event sequences 3
2.4. Event sequence categories considered in safety approach 3
2.5. Risk limit 5

3. ELEMENTS OF THE RISK-INFORMED FRAMEWORK 6
3.1. Initial design development 6
3.2. Probabilistic Risk Assessment 7
3.3. Evaluate risk against risk limit and identify “required safety functions” 8
3.4. Evaluate the role and perform safety classification of plant equipment 8
3.5. Deterministic safety analyses 10
3.6. Evaluation of defense-in-depth adequacy 10

4. SUMMARY 12

References 13

List of Figures

Figure 1: Safety classification for plant equipment (a structure, system, or component). 3
Figure 2: A conceptual and simplistic risk limit. 6
Figure 3: Identification of prevention and mitigation functions illustrated on risk limit for an above-target event sequence. 9

List of Tables

Table 1: IAEA's Defense-in-depth (DiD) levels and a summary of their purpose [3]. 2
Table 2: Plant states considered in design. 4
Table 3: Process for evaluation of Defense-in-Depth adequacy 11

List of Acronyms

AOO	Anticipated Operational Occurrence
CNRA	Committee on Nuclear Regulatory Activities
CFD	Computational Fluid Dynamics
DEC	Design Extension Condition
DBA	Design Basis Accident
DiD	Defense-in-Depth
GIF	Generation-IV International Forum
IAEA	International Atomic Energy Agency
LOP	Lines of Protection
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NO	Normal Operation
OPT	Objective Provision Tree
PES	Practically Eliminated Situation
PIRT	Phenomena Identification and Ranking Table
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
QSR	Qualitative Safety-features Review
RSWG	Risk and Safety Working Group
WGSAR	Working Group on Safety of Advanced Reactors

(This page has been intentionally left blank)

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 defense-in-depth (DiD) assessment as an integral part of the process to ensure compliance with safety design criteria and establish links between the 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 this framework [1] was developed based on the U.S. regulatory codes and standards, this position paper includes broader considerations to generalize the approach for other safety frameworks mainly based on the 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 by integrating the deterministic input and risk insights to identify and classify the event sequences in each category,
- define the characteristics of a generic risk limit to evaluate the event-sequences against the regulatory requirements and safety goals,
- establish a process to classify the plant equipment based on their risk-significance and the role in plant safety (for 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 and the responding plant equipment with the DiD levels, and
- help with classification of very-low-frequency event sequences as residual risk, including identification of high-consequence cliff-edge effects to ensure that the event sequences with potential for unacceptably large or early releases are practically eliminated.

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

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

recognized IAEA terminology and corresponding definitions are preferred throughout this position paper. The phrases and sentences quoted from the IAEA safety glossary [2] and the key concepts quoted from the IAEA safety standards are shown in *italic letters*. The phrases and key concepts borrowed from other references are quoted and referenced as introduced.

2.1. Defense-in-depth

DiD 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, defense in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combination of failures that could give rise to significant harmful effects are of very low probability* [2].

Table 1: IAEA's Defense-in-depth (DiD) levels and a summary of their purpose [3].

DiD level	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 features, safety systems and procedures.*
4	Prevent the progress, and mitigate the consequences, of accidents that result from failure of the third level of defense to avoid large or early releases of radioactive material.
5	Mitigate radiological consequences of radioactive material release that could potentially result from an accident condition.

NOTE: The risk-informed approach retains the "cascading failure" concept to capture the accidents progressing to successive levels, and it could also potentially identify a "non-cascading" event (such as a DBA initiator).

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 the terminology differs significantly in each country, the plant equipment classification and corresponding definitions are based on the IAEA safety standards and glossary [2] to establish an internationally recognized common vocabulary.

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 "*an item important to safety that is not part of a safety system or a safety feature for design extension conditions*" [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 for design extension conditions* that inherently have, or are designed to perform, a safety function for design extension conditions to mitigate the consequences of malfunction or failure of *safety* systems.

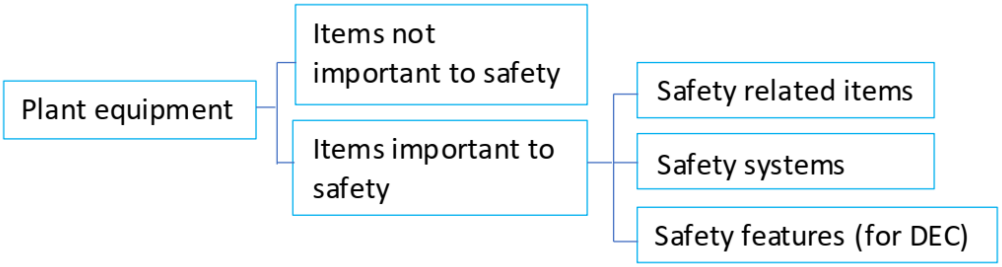


Figure 1: Safety classification for plant equipment (a structure, system, or component).

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 caused by 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 the 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 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, typically the safety related items are considered to prevent AOOs from leading to accident conditions. The safety systems may also be capable of responding to an AOO and their performance should be designed accordingly.
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 safety systems.	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.
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 and are typically more complex than DBAs (with some potential overlap). Despite their low frequency of occurrence, they are still considered in the design.	Once the safety-classification of the plant equipment is completed, independent safety features for DEC (to the extent practicable) are considered to prevent "severe plant conditions" [4], or mitigate and limit their consequences to within the regulatory dose limits. DEC mitigation may also rely on availability of some safety systems if they are not damaged by, and their failure is not part of, the event sequence under consideration.

* Safety function of the barriers against the release of radioactivity 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 design criteria and evaluated via conservative methods [4]. 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]" [4]. Although DECs are evaluated in accordance with the best estimate methodology, the safety function of the responding plant equipment and other intrinsic design 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 [4]. The design basis conditions complemented by the design extension conditions (DEC) constitute the plant design envelope.

The event sequences that are not part of the design envelope are not considered in further analysis consistent with 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 still required to be ruled out from the design through a robust safety demonstration that shows they are either physically impossible or extremely unlikely with a high degree of confidence [4].

2.5. Risk limit

A risk-informed approach uses a set of frequency-consequence criteria to represent the risk and establish a correlation between the permissible dose and frequency limits when evaluating the event sequences. Such a generic correlation, referred to as the "risk limit" 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 the overall structure of the risk limit will differ as well. The simplistic representation shown in Figure 2 can accommodate these variations without an impact on the other concepts introduced here.

The risk is multiplication of the frequency and consequence (with the unit of "dose per plant year"). In Figure 2, the acceptable risk is delineated by the red "risk limit" against which the safety significance of, and relative safety margins for, the individual event sequences are evaluated. The risk limit provides a tool to compare the risk from an event sequence with the applicable regulatory requirements and allows the plant conditions to be 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 potentially high consequences.

Once the system safety architecture is defined, the designer must prove that, for all the "design basis conditions" and *design extension conditions*, the system response allows the risk to be kept within the acceptable domain—below the "risk-limit"—with margin. Safety significance of the involved plant equipment is also evaluated so that their classification is consistent with the role they play to keep the risk below the "risk-limit" for all event sequences, again with margin.

[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 does not apply to some Generation-IV designs, the term "severe plant conditions" is used consistent with the terminology adopted in [4]. Its proposed definition is "a postulated degraded plant state where the first barriers to the release of substantial amount of radioactivity are ineffective and large and early releases are prevented by the last designed barrier."

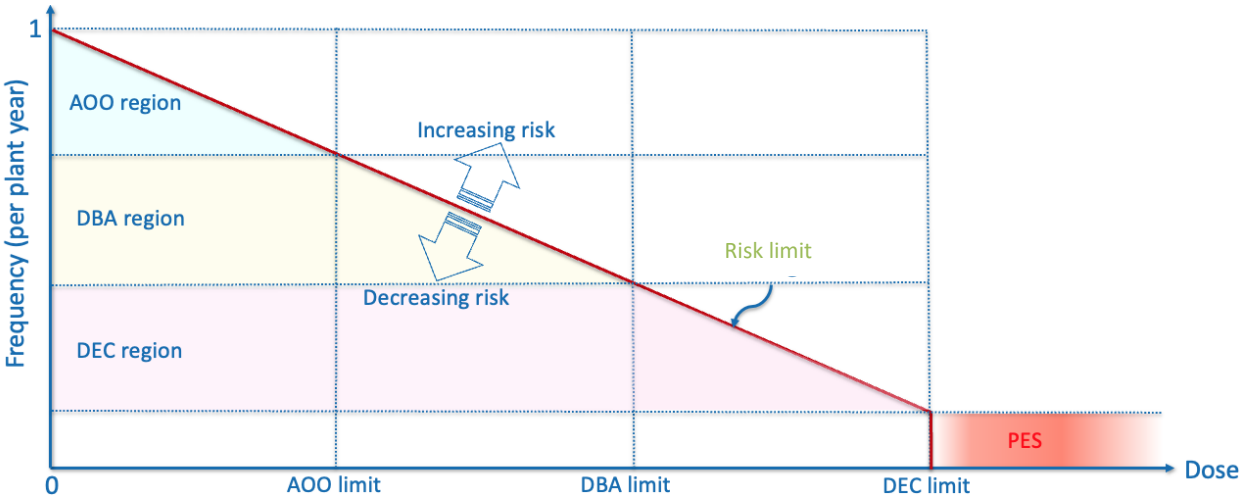


Figure 2: A conceptual and simplistic risk limit.

The domain beyond the vertical portion of the "risk-limit" indicates that the residual risk event sequences with potential large releases (beyond the regulatory limit) will need to be practically eliminated consistent with GIF safety goal for "elimination of the need for off-site emergency response."

3. ELEMENTS OF THE RISK-INFORMED FRAMEWORK

A 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 conditions a design can be exposed to. The approach can be technology-neutral and can 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 a risk informed process to identify and categorize the event sequences and to support safety classification of the plant equipment are summarized below.

3.1. Initial design development

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 and the tools that can assist it may include:

- Definition/refinement of the safety approach using Qualitative Safety-features Review (QSR) [4] as a preparatory "checklist" method for systematic review of design characteristics and requirements to ensure desired safety attributes, identification and fine-tuning of design features to meet the safety design criteria,
- Categorization and ranking of the relevant phenomena in terms of their safety importance and state of knowledge in a Phenomena Identification and Ranking Table (PIRT) [4] to evaluate the knowledge base and identify gaps for the deterministic safety analyses and probabilistic risk assessments,
- Identifying the specific provisions to fulfil the fundamental safety functions at each DiD level using tools like Objective Provision Tree (OPT) [4], and
- Assessment of the effectiveness of the Lines of Protection (LOP) [4] for the set of safety

[3] A safety function (potentially among many) required to maintain the risk from one or more event sequences below the risk limit while also meeting the "cumulative risk targets" such as the annual dose limit and/or the risk for early/latent fatalities.

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 collectively 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.

These tools also facilitate 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, based on expert judgment and risk insights from prior experience. Although this first list will likely be incomplete, the list is gradually revised and expanded throughout the design iterations including the risk-informed input as discussed in following sections.

3.2. Probabilistic Risk Assessment

A Probabilistic Risk Assessment (PRA), also known as Probabilistic Safety Assessment (PSA), provides a structured means to answer the basic questions: What can go wrong and how likely is it to occur? The PRA is traditionally used for Generation-II and -III reactors to evaluate core damage frequency and assess the consequences of bounding accident sequences (such as a large-break loss-of-coolant accident). As part of a risk-informed approach, PRA involves the analysis of full range of event sequences for consequence assessments in the entire frequency spectrum to support identification and implementation of the risk management strategies. These risk insights can then supplement the traditional 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, as new reliability data from component testing or prior operational experiences becomes available, and the site is selected. The PRA model is 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 analyses event sequences and assesses the frequency of each event sequence including internal events, human errors, and external hazards. The modelled event sequences 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.

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. They are assigned to an event sequence category (AOO, DBA, or DEC) based on their frequency of occurrence per plant-year. Event sequences with frequencies below the residual risk limit 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 risk limit and identify "required safety functions"

The results of the PRA for all event sequences are weighed against the risk limit (introduced in Figure 2 as a simplistic example) to focus the attention on the safety-significant event sequences, to identify the ways for their prevention, and identify possible means to address their consequences. The risk is evaluated 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 studies.

The primary purpose here is to evaluate the risk from each event sequence including the response of the involved plant equipment. Another objective is to identify the design features and plant equipment that are responsible for (1) preventing or limiting radiological releases for each event sequence and (2) 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 safety significance of plant equipment in support of their safety classification as discussed next.

The full set of AOOs, DBAs and DECs are then 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 safety goals for AOOs are to prevent them from progressing to accident conditions, posing challenges to the *safety systems*, and exceeding the associated dose limits. The safety goals for DBAs and DECs are both preventing them by reducing their likelihood through improved reliability, and mitigating them by reducing their consequences within respective dose limits.

A risk-informed approach highlights and informs the necessary considerations of both prevention and mitigation functions. The impact of a "required safety function" is illustrated conceptually in Figure 3 with the horizontal arrow for the mitigation function and vertical 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 in the next section.

3.4. Evaluate the role and perform safety classification of plant equipment

The purpose of this evaluation is to identify design features and plant equipment that are responsible for keeping the event sequences well below the risk limit with margin. In addition to the predicted risk for each event sequence, the integrated risk for all event sequences is used to evaluate the role of the involved plant equipment (including the barriers) and other intrinsic design characteristics.

For each "required safety function" identified in previous section, the key plant equipment or intrinsic design characteristic are identified as safety-significant and broadly defined as "*items important to safety*." The requirements for these items 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).

In contrast, a plant equipment is considered risk-significant if its safety function is essential to keep the risk from one or more event sequences below the "risk limit". 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-

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

significant if the integrated risk for all event sequences with the failed plant equipment exceeds the "cumulative risk targets". A risk-significant plant equipment that may perform a safety function for prevention or mitigation is depicted in Figure 3.

The risk-significant plant equipment typically includes the key *safety systems* for DBA and *safety features* for DEC. While the safety-significant plant equipment generally enhances the safety of a design (to reduce an acceptable but dominant risk[5], for example), the safety function of a risk-significant plant equipment is essential to achieve the overall risk-informed design (without it, the risk would be unacceptable).

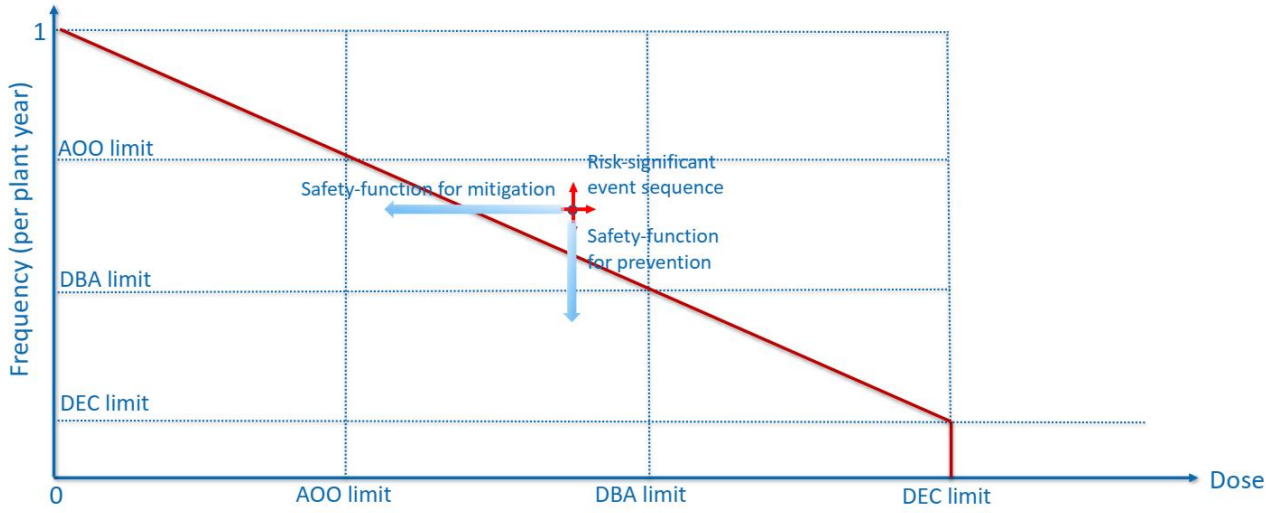


Figure 3: Identification of prevention and mitigation functions illustrated on risk limit for an above-target event sequence.

The plant equipment safety classification process can be as described below:

- Each risk-significant event sequence (those that land above the risk limit) is examined to determine which plant equipment or intrinsic design characteristics are available to fulfil the required safety functions. Then, one or more of available plant equipment or intrinsic design characteristics are selected to perform each safety function.
    - The minimum set of specific plant equipment that can be solely relied on during DBAs are classified as *safety systems*.
    - The minimum set of specific plant equipment or intrinsic design characteristics that can be relied on during DECs are classified as "*safety feature for DEC*" (an item or process that is designed to perform a safety function, or inherently has that safety function).
- The remaining plant equipment are further evaluated to determine if they make significant contributions to maintain the "cumulative risk targets".
- 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 an item *important to safety*.

[5] When the risk is below the "risk-limit", but uncomfortably close to it in comparison to other event sequences.

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.

To repeat, a risk-significant plant equipment reduces the frequency or consequence of a risk-significant event-sequence so that the associated risk falls under the risk limit curve. A safety-significant plant equipment further reduces the frequency or consequence of an event-sequence mainly to address the dominant risk or address uncertainties in frequency and consequence predictions.

3.5. Deterministic safety analyses

The deterministic safety analyses involve 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 include 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 defense and degree of their independence, and to confirm the design basis for *items important to safety*.

The bounding AOO, DBA and DEC events (either a single initiating event or a complex sequence) 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 regulatory requirements.

- For each DBA, the 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, the 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 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 they are not damaged by, or their failure is not part of, the event sequence under consideration. The DECs are usually considered in the deterministic safety analyses using the best-estimate methods, although conservative approach is also considered in some countries to add additional robustness in the design.

3.6. Evaluation of defense-in-depth adequacy

This step ensures that the proposed plant design and safety approach maintain sufficient layers of protection (defense-in-depth) against accidents. After identifying the event sequences and classifying the plant equipment, the designer evaluates whether the combination of preventive and mitigative measures provides reasonable assurance of safety — even if one layer fails. The assessment checks that no single barrier or function is overly relied upon, that risk insights support the adequacy of protections, and that residual risk remains acceptably low consistent with defense-in-depth principles.

This involves confirming that the risk limit and “cumulative risk targets” for all event sequences are met in all DiD levels, also 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 safety function so that no single *plant equipment* or *safety feature*, no matter how robust

and reliable, is exclusively relied on to achieve the overall safety design goals. The process for evaluation of DiD adequacy is outlined in Table 3.

DiD is deemed to be adequate when:

- DiD guidelines to achieve the safety design goals listed in Table 3 are satisfied,
- margins against the risk limit are sufficient and the "cumulative risk targets" are met,
- role of plant equipment in prevention and mitigation at each layer of defense is established,
- 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 prevention measures),
- independence of design features at each layer of defense is sufficient so that the same *plant equipment* (*safety system* or *safety feature* for DEC) is not primarily responsible for the plant safety in multiple DiD layers), and
- design margins in plant capabilities are adequate to address the uncertainties identified in the PRA as well as the deterministic and phenomenological analyses.

Programmatic elements[6] complement this process 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.

Table 3: Process for evaluation of Defense-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 defense-in-depth. This can also be achieved by preventing the progression of such accidents into a "severe plant condition."

[6] Programmatic elements of defense-in-depth, as introduced in [1], refer to the institutional and administrative controls, procedures, and programs to support the safe operation of a reactor (beyond physical plant structures, systems, and components) and to act as an additional layer of safety to compensate for potential design or operational shortcomings.

Outcomes of this effort 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.

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 defense-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 risk limit 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 defense-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 aims to broaden its applicability by generalizing it for other regulatory frameworks mainly based on the 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 far more significant effort over many years requiring very substantial resources beyond the means of the GIF RSWG.

References

[1] Nuclear Energy Institute, "*Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development (NEI 18-04 Rev. 1)*," Nuclear Energy Institute, Retrieved from https://www.nrc.gov/docs/ML1924/ML19241A472.pdf, Washington DC, 2019.

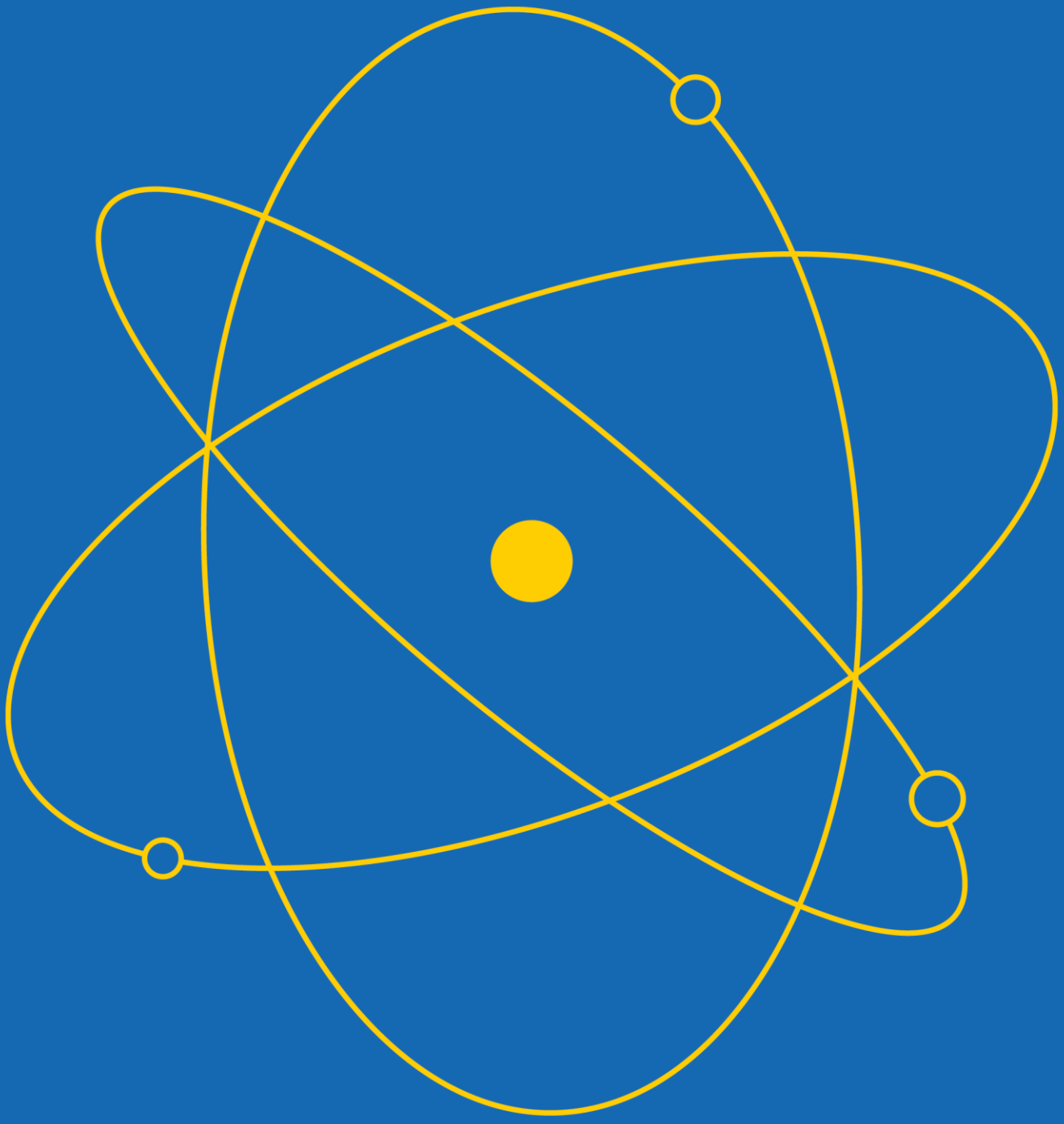
[2] International Atomic Energy Agency, "*IAEA Nuclear Safety and Security Glossary, 2022 (interim) edition*", IAEA, Vienna, 2022.

[3] International Atomic Energy Agency, "*Safety of Nuclear Power Plants: Design (SSR-2/1 Rev. 1)",* IAEA, Vienna, 2016.

[4] Generation IV International Forum Risk and Safety Working Group, "*Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems"*, GIF, Paris, 2021.

THE GENERATION IV INTERNATIONAL FORUM

Established in 2001, the Generation IV International Forum (GIF) was created as a co-operative international endeavor seeking to develop the research necessary to test the feasibility and performance of fourth generation nuclear systems, and to make them available for industrial deployment by the 2030s. Under the new 2025 GIF Framework Agreement, GIF brings together countries, as well as Euratom, representing 27 EU member states, to co-ordinate research and develop these systems. GIF has selected six reactor technologies for further research and development: the gas-cooled fast reactor (GFR), the lead-cooled fast reactor (LFR), the molten salt reactor (MSR), the sodium-cooled fast reactor (SFR), the supercritical-water-cooled reactor (SCWR) and the very-high-temperature reactor (VHTR).



A report produced by

25 YEAR ANNIVERSARY
GEN IV INTERNATIONAL FORUM
Expertise | Collaboration | Excellence

www.gen-4.org

RSWG