INL/EXT-21-64077
Revision 0

FY 2021 GIF-RSWG and WGSAR Status Report

August 2021

James C. Kinsey

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance, LLC

INL/EXT-21-64077
Revision 0

FY 2021 GIF-RSWG and WGSAR Status Report

James C. Kinsey

August 2021

Idaho National Laboratory
Advanced Reactor Technologies
Idaho Falls, Idaho 83415

http://www.ART.INL.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

INL Regulatory Development Program

FY 2021 GIF-RSWG and WGSAR Status Report

INL/EXT-21-64077
Revision 0

August 2021

Approved by:

Jason A Christensen	08/23/2021
Jason Christensen Regulatory Development Engineer	Date
Gerhard Strydom	8/23/2021
Gerhard Strydom INL ART GCR National Technical Director	Date
Michelle Sharp	8/24/2021
Michelle T. Sharp INL Quality Assurance	Date

Page intentionally left blank

SUMMARY

This report provides an end-of-year summary that reflects the progress and status of United States activities supporting the Generation-IV International Forum's Risk & Safety Working Group and the international regulators associated with the Working Group on the Safety of Advanced Reactors. This effort has commenced with the development of a technology-neutral, risk-informed approach for the selection of licensing basis events and the assessment of defense in depth for Gen-IV reactor technologies. These U.S. activities are being managed by Idaho National Laboratory on behalf of the U.S. Department of Energy.

Page intentionally left blank

CONTENTS

SUMMARY vii
ACRONYMS x
1. PURPOSE 1
2. OBJECTIVES 1
3. BACKGROUND 2
3.1 Risk and Safety Working Group 2
3.2 Working Group on the Safety of Advanced Reactors 2
3.3 U.S. Contribution 2
3.4 Planned Output Document 3
4. SUMMARY OF FY 2021 ACTIVITIES 3
4.1 Coordinated GIF-RSWF and WGSAR Meetings (September, October 2020) 3
4.2 Development of Position Paper to Address Selected Key Issues 3
4.3 Draft Report Addressed at GIF—RSWG and WGSAR Meetings (April 2021) 4
5. NEXT STEPS 4
6. REFERENCES 4
ENCLOSURE 1 5

ACRONYMS

AOO	Anticipated Operational Occurrence
BEPU	Best-estimate plus uncertainties
CFD	Computational fluid dynamics
DBA	Design Basis Accident
DEC	design extension condition
DiD	defense in depth
Gen-IV	Generation IV
GIF	Generation-IV International Forum
IAEA	International Atomic Energy Agency
LBE	licensing basis events
LOP	Lines of Protection
LWR	light-water reactor
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission
PES	practically eliminated situations
PRA	probabilistic risk assessment
RSWG	Risk & Safety Working Group
SSC	structures, systems, and components
WENRA	Western European Nuclear Regulators Association
WGSAR	Working Group on the Safety of Advanced Reactors
U.S.	United States

Page intentionally left blank

FY 2021 GIF-RSWG and WGSAR Status Report

1. PURPOSE

This report provides an end-of-year summary that reflects the progress and status of United States (U.S.) activities related to its proposal for a joint effort engaging the Generation-IV International Forum's Risk and Safety Working Group (GIF-RSWG) and the international regulators associated with the Working Group on the Safety of Advanced Reactors (WGSAR). This effort has commenced with the development of a report that describes a technology-neutral, risk-informed approach for the selection of licensing basis events (LBE) and the assessment of defense in depth (DiD) for Generation IV (Gen-IV) reactor technologies.

The approach being considered recognizes that advanced reactor technologies provide an opportunity for design simplifications and improved safety through an emphasis on the utilization of inherent and passive safety features. The goal is to achieve safety that is built into the design, not added on, by relying on a combination of deterministic and risk-informed safety approach to implement the DiD principles.

The approach is being developed in coordination with GIF-RSWG and the WGSAR to establish a harmonized structure that would allow for both reactor developers and regulators to assess the passive and inherent safety attributes of those technologies more consistently and effectively. The U.S. activities summarized in this report are being managed by Idaho National Laboratory, with additional support from Argonne National Laboratory, on behalf of the U.S. Department of Energy.

2. OBJECTIVES

Several current regulatory review processes are based primarily on light-water reactor (LWR) technology and focus on prescriptive, deterministic approaches, active systems, and associated DID principles. Since some Gen-IV systems are pursuing demonstration/deployment within the next decade, a more efficient, systematic, and predictable process leading to an early resolution of fundamental technical issues is needed to support the efficient licensing and commercialization of Gen-IV technologies and to reduce regulatory uncertainties to developers, investors, regulators, and potential owner/operators.

The objectives and anticipated benefits of this effort are expected to include:

- Establishing a process that allows for considerations and flexibilities regarding the improved safety margins and advanced design approaches associated with advanced non-light-water reactors while maintaining protection of the public
- Establishing an agreed upon risk-informed approach to event selection, providing a foundation that technology developers can implement early in the design to avoid costly modifications late in the regulatory review and deployment process
- Providing a framework for a transparent and repeatable way to assess the adequacy of DiD measures, including addressing the concept of "practical elimination."

3. BACKGROUND

3.1 Risk and Safety Working Group

The RSWG was formed to promote a homogeneous and effective approach to assuring the safety of Gen-IV nuclear energy systems. The overall success of the Gen-IV program depends on, among other factors, the ability to develop, demonstrate, and deploy advanced system designs that exhibit excellent safety characteristics. While the RSWG recognizes the excellent safety record of nuclear power plants currently operating in most GIF member countries, it believes that progress in knowledge and technologies and a coherent safety approach hold the promise of making Gen-IV energy systems even safer and more transparent than the current generation of plants. The RSWG goal most closely aligned with this effort is to: *Promote a consistent approach on safety, risk, and regulatory issues between Generation IV systems.*

3.2 Working Group on the Safety of Advanced Reactors

WGSAR activities support the Nuclear Energy Agency (NEA) in achieving its goals to "address safety issues associated with new technologies and reactor designs" and to "help maintain an adequate level of capability and competence in member countries necessary to ensure the safety of future nuclear facilities and activities." In this context, the mandate of the WGSAR is to exchange information and experience from licensing and oversight of past and current nuclear facilities.

The WGSAR provides regulatory perspectives through the issuance of technical reports discussing areas in which additional or revised regulatory framework and licensing approaches, including safety research, may be needed to facilitate the effective regulation of advanced reactors and to develop common understanding and approaches. Its involvement in this joint effort is most closely associated with its working method of sharing information and experience on the regulation of advanced reactors to facilitate a cooperative approach to identify key regulatory issues, promote a common resolution, and document commendable practices.

3.3 U.S. Contribution

A technology-neutral, risk-informed, performance-based approach for LBE selection and safety classification of structures, systems, and components is being developed to address the key Gen-IV reactor development and licensing issues. The proposed approach is based on the foundations and key attributes of the Licensing Modernization Project approach developed in the U.S. and endorsed by U.S. industry stakeholders. This approach was approved in 2020 by the Nuclear Regulatory Commission (NRC) for implementation in the U.S. via the issuance of NRC Regulatory Guide 1.233. Adaptation and adoption of the key attributes and concepts within this approach on a more global scale would provide an expanded foundation on which the safety bases and design margins of Gen-IV technologies can be evaluated.

The implementation of the approach description established through RSWG and WGSAR interactions is intended to maintain an alignment of the Gen-IV concepts with the multiple levels of defense currently reflected in various international standards (International Atomic Energy Agency [IAEA], Western European Nuclear Regulators Association, Committee on Nuclear Regulatory Activities, etc.) while allowing flexibility for advanced reactor concepts to take full advantage of their passive and inherent safety attributes.

3.4 Planned Output Document

A joint RSWG-WGSAR report describing the approach is being developed over the course of this joint initiative, initially based on the U.S. contribution to this effort via the GIF- RSWG in close coordination with the WGSAR. A detailed summary of the progress in developing and issuing that report is provided in Section 4 below. Broader GIF system steering committee involvement for design-specific input to the process may be arranged through RSWG. Since both RSWG and WGSAR also include observers from IAEA, the consistency of the proposed approach with IAEA's safety standards and guidelines can be captured, including both the designer and regulatory perspectives.

4. SUMMARY OF FY 2021 ACTIVITIES

FY 2021 activities continued throughout the year, and included the following areas of most significant interaction:

4.1 Coordinated GIF-RSWF and WGSAR Meetings (September, October 2020)

The U.S. participated in two separate but coordinated GIF-RSWG and WGSAR meetings. The GIF-RSWG meeting was held on September 30, 2020, and the WGSAR meeting was held on October 15, 2020. (It is noted that both meetings were attended virtually due to ongoing travel restrictions.)

Regarding this joint regulatory report development effort, the primary purpose of those meetings was for the U.S. members to update members regarding the most recent GIF-RSWG dialogue and remaining open issues associated with the key portions of the proposed risk-informed and performance-based approach. During the above update meetings, it was noted that a consensus among GIF-RSWG members could not be established regarding the content of the draft report developed and discussed throughout 2020. In particular, there are ongoing challenges in the following areas within the overall approach:

- Terminology and definitions
- Handling of design extension conditions and practically eliminated situations.

In follow-up discussions within the GIF-RSWG, it was decided to scale down the effort to development of a "position paper" (see Enclosure) that outlines the foundation and main elements of a risk-informed approach. Once there is an agreement over the position paper content between RSWG and WGSAR, additional details and layers can be added onto it in coming years.

4.2 Development of Position Paper to Address Selected Key Issues

A position paper was developed that introduces foundational concepts and provides an outline of a risk-informed approach that combines both deterministic and probabilistic insights into the decision-making process in a complementary way to inform the safety design and demonstrate alignment with DiD principles. In particular, the foundational portions of the approach reflected in the position paper aim 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 broad structure of a generic frequency-consequence target to classify and 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 including the consideration of the prevention and mitigation functions of the plant equipment within each event sequence evaluated

- Support deterministic analysis of the 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 as defined by IAEA and Western European Nuclear Regulators Association (WENRA)
- Establish the process for treatment of low-frequency event sequences as residual risk, including the consideration of high-consequence cliff-edge effects to help identify practically eliminated situations.

4.3 Draft Report Addressed at GIF—RSWG and WGSAR Meetings (April 2021)

The draft position paper content was discussed during the regular bi-annual GIF-RSWG meeting held on April 19, 2021. Additional member insights and considerations were collected, and an updated and final draft version of the paper was distributed for near-term GIF-RSWG member concurrence, with an action to provide any remaining inputs by July 31, 2021. A brief status update regarding the revised approach and timeline was provided to the WGSAR during their regular bi-annual meeting held on April 21, 2021.

5. NEXT STEPS

The enclosed position paper, reflecting the consensus of GIF-RSWG members, was distributed to the WGSAR for review and comment on August 4, 2021. It is expected that initial WGSAR inputs and insights will be available and can be discussed during the next set of annual coordinated GIF-RSWG and WGSAR meetings, nominally scheduled for October 2021. The goal is to achieve WGSAR and GIF-RSWG consensus on the position paper content by the end of calendar year 2021. Consensus could then be followed by the development and incorporation of additional details and layers in coming years.

6. REFERENCES

1. 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).
2. "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).
3. Task Force on Safety Design Criteria, Generation IV International Forum (GIF), https://www.gen-4.org/gif/jcms/c_93020/safety-design-criteria.
4. U.S. Nuclear Regulatory Commission Regulatory Guide 1.233, Revision 0, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-water Reactors." (June 2020), ADAMS Accession No. Ml200911698.
5. International Atomic Energy Agency (Rev. 1), "Safety of Nuclear Power Plants: Design." Safety Standard Series No. SSR 2/1, IAEA, Vienna (2012).

ENCLOSURE 1

A Risk-Informed Approach for Gen-IV Systems

INTRODUCTION

Novel aspects of numerous advanced reactors require 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 alternative searches of event sequences by examining both their probability and consequences to understand the risks and identifying additional requirements or regulatory actions as needed. 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 the safety design criteria and establish links between *required safety functions* and design requirements.

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 DID principles. In particular, 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,
- Assess the alignment of event sequence categories considered in design with the DiD levels as defined by IAEA and WENRA, and
- Establish the process for treatment of low-frequency event sequences as residual risk, including the consideration of high-consequence cliff-edge effects to help identify practically eliminated situations.

FOUNDATIONAL CONCEPTS

In order to achieve consensus among RSWG and WGSAR members, the IAEA terminology and corresponding definitions are preferred throughout this paper. The sentences quoted from the IAEA safety glossary[1] and the key concepts introduced in this paper are included in *italic* letters.

* 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.

Defense-in-Depth

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.*" [1]

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. Defense-in-Depth (DiD) levels and their purpose.

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 systems* and procedures.
4	Prevent the progress, and to mitigate the consequences, of accidents that result from failure of the third level of defense 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-based structure retains the "cascading failures" concept to successive levels. A risk-informed approach would address this consideration but could also potentially identify "non-cascading" event sequences that might otherwise be missed.

Plant Equipment Classification

The terminology for the safety classification of the plant equipment adopted in this paper is shown in Figure 1. Since this terminology differs significantly in each country, the plant equipment classification and corresponding definitions are based on IAEA safety standards and glossary [1] to establish an internationally recognized common terminology.

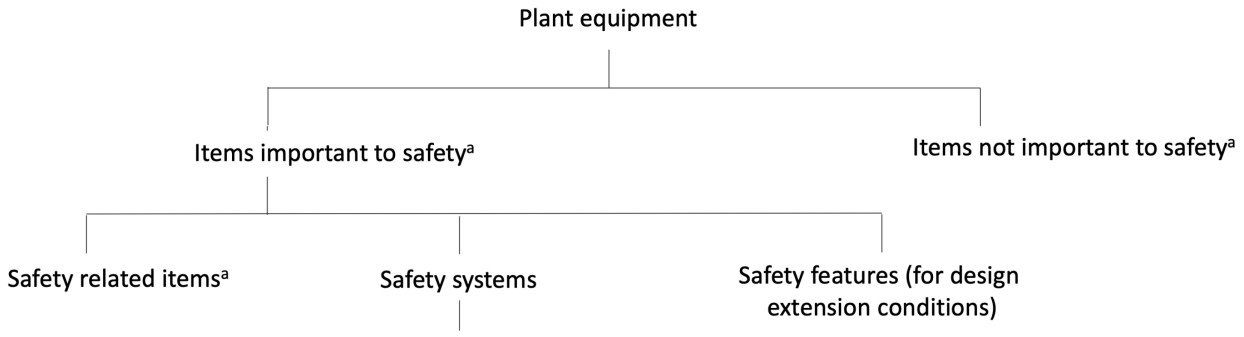

Figure 1. Safety classification for plant equipment.

[a]An "item" is a Structure, System, or Component (SSC). Throughout this paper, "plant equipment" and "SSC" terms are used interchangeably.

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.*"[1] It is primarily intended to prevent an anticipated operational occurrence from leading to an accident.
- 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.*"[1]
- 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*.

Initiating Events and Event Sequences

An event sequence is comprised of an initiating event, a sequence of involved plant equipment response, and a stable end-state. 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, as well as their stable end state, then depend on additional failure assumptions for the involved plant equipment in these sequences. Therefore, depending on the plant's response, the same initiating event could lead to different categories of event sequences introduced in Table 2 based on the mean frequency of occurrence of each event sequence per plant-year.

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 [1] 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 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.

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*.* Appropriate design rules and the applicable criteria are also established for DECs, in addition and complementary to those for DBAs.[2]

The residual risk event sequences with sufficiently low frequency of occurrence are not considered in further analysis due to implementation of defense-in-depth principles. Among them, 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, 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.[2] The failure of the 4th level of DiD is part of residual risk but not a part of practically eliminated situations to assure that there are no such cliff-edge effects with unacceptable spatial or temporal consequences.

---

* 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 Gen-IV systems such as VHTR and MSR, the term "*severe plant conditions*" is used consistent with the approach adopted in Reference 2.

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 that are classified as *items important to safety*.
Anticipated Operational Occurrence (AOO)	*A deviation of an operational process from normal operation that is 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.*[1] In this paper, the 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 providing an acceptable plant response and outcome for AOOs.
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.*[1] DBAs are infrequent event sequences that are 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 established, 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 that are not considered for design basis accidents, but that are 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.*[1] 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 a 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, only the specific, 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 included in this table.

Alignment of Event Sequence Categories and Plant Equipment Classification with DiD Levels

Alignment of DiD levels with the event sequence categories considered in design and responding plant equipment classification is shown in Table 3 along with the corresponding recommended analysis methodology. It is important to recall that, within the context of a risk-informed approach, the AOO, DBA, and DEC categories in column 2 of Table 3 are for the whole event sequences, not just the initiating events. In that sense, different categories of event sequences can be built based on the same initiating event depending on additional plant equipment failure assumptions.

Table 3. Alignment of plant states and plant equipment classification with DiD levels.

DiD level	Plant state	Analysis methodology	Responding plant equipment	
1	NO	Conservative	*Items not important to safety*	
2	AOO	Conservative, including best estimate plus uncertainties (BEPU)	*Safety related items*	*Items important to safety*
3	DBA	Conservative, including BEPU	*Safety systems*	
4	DEC	Mainly best estimate, BEPU is also considered (includes *severe plant conditions* if they result from the event sequence)	*Safety features*	

The practically eliminated situations (PES) are distinctly different from the other event sequences in the residual risk domain in a way that their exclusion from the design may depend mainly on dependability of prevention mechanisms requiring a robust demonstration of their reliability with high degree of confidence, backed with surveillance, inspection, and periodic testing procedures. When warranted, prevention of PES should be evaluated using the BEPU or conservative approach, supported with a robust safety demonstration, to justify their exclusion from the design and to assure that there are no associated cliff-edge effects resulting from this exclusion.

Frequency-Consequence Target

A 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 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. Also, as noted in the WENRA framework, 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 any impact on the other concepts and approach introduced in this 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 iso-risk line against which the risk and safety significance of, and relative safety margins for, the individual event sequences are evaluated. Although the shape of iso-risk line will vary and may look more like a staircase, its shape is generally determined to balance the risk profile across the entire frequency spectrum and minimize the integral risk for the whole plant design consistent with the national regulatory limits.

The *frequency-consequent 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 iso-risk line 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 highly hypothetical accident sequences and *severe plant conditions*.

Once the system safety architecture is defined, the designer must prove that, for all the design basis and design extension conditions which the plant must deal with, the system response allows the corresponding risk to be kept within the tolerable domain—below the iso-risk line 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 iso-risk line for all event sequences, again with margin. The vertical portion of the iso-risk line is intended to imply that there should be no acceptable frequency for large releases.

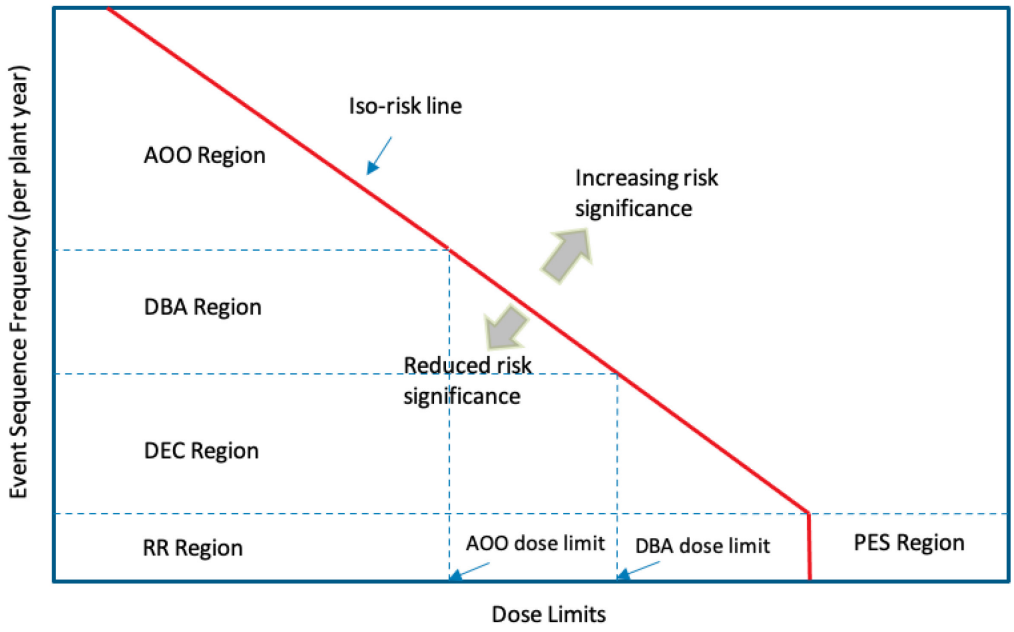

Figure 2. Frequency-Consequence Target.

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. It can also ensure that the plant equipment that perform a *required safety function*[*] 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. The process is repeated for each design phase until the list of AOO, DBA and DEC event sequences becomes stable and considered final. 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 other *safety features* that are key for design completeness in compliance with DiD principles.

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)[2] for identification and fine-tuning of design features to meet the safety design criteria,
- Development of Phenomena Identification and Ranking Table (PIRT) [2] to evaluate and build sufficient knowledgebase for the deterministic safety analyses and probabilistic risk assessments,

---

* A function that is required to be fulfilled to maintain the risk from one or more design basis or design extension conditions 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.

- Identifying the specific provisions to fulfill the *required safety functions* at each DiD level using tools like Objective Provision Tree (OPT) [2], and
- Assessment of the effectiveness of the Lines of Protection (LOP) [2] 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).

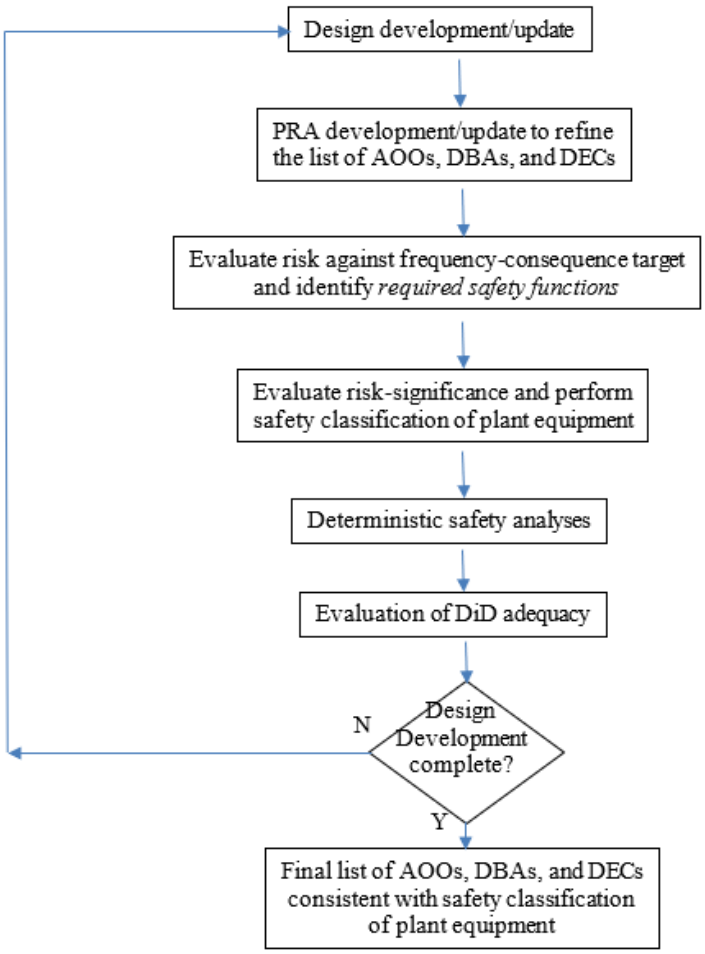

Figure 3. Process for selection of AOOs, DBAs, and DECs.

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.

Early in the design development process, the first 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 [3], 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.

PRA Development/Update to Refine the List of AOOs, DBAs, and DECs

The Probabilistic Risk Assessment (PRA) 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 LWRs 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. Therefore, the PRA model is often updated to reflect changes in the design and system configuration. And PRA results, in return, influence the design process by contributing to key decisions and adopting 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 typically accommodated in a design through additional safety margins. Leaving big margins for safety is, of course, expensive and it may keep the focus away from dominant risk contributors. The PRA can help identify the risk-significant uncertainties and their sources to help the developers achieve an optimized design by considering safety, reliability, and economic factors.

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. 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, a stable end state, and dose consequences if a radiological release is anticipated. Each of these families is assigned to an event sequence category (AOO, DBA, or DEC) based on mean event sequence frequency of occurrence per plant-year. Event sequences with frequencies close to the residual risk 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 the last step. 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.

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 from all event consequences 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. Unresolved uncertainties should be addressed as part of risk-informed evaluation of DiD as the last step of the risk-informed process.

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*[*] 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 and to mitigate their consequences from exceeding the associated offsite 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.

Historical approaches to event sequence identification and its treatment in the plant design have tended to focus primarily on mitigation, with less emphasis on prevention. Proposed 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 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.

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). The safety-significant plant equipment are broadly defined as the *items important to safety* in a way that they perform a general safety function necessary to achieve adequate DiD.

---

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

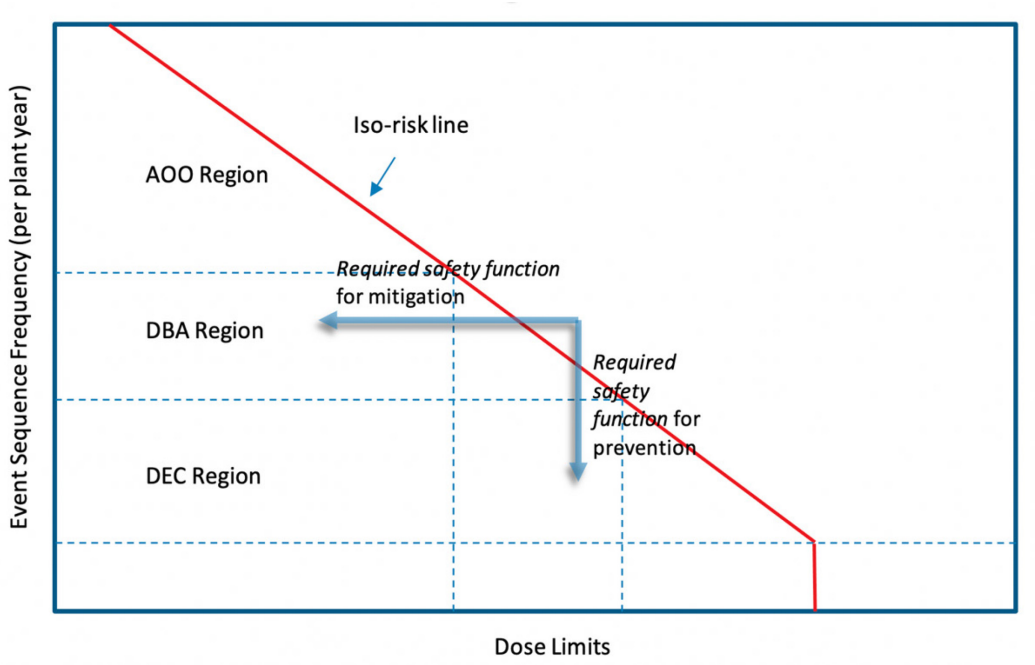

Figure 4. Identification of prevention and mitigation functions illustrated on frequency-consequence target for an above-target event sequence.

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 inside the *frequency-consequence target* based on mean frequencies and consequences. 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. While the safety-significant plant equipment enhances the safety of a design (to reduce 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 *frequency-consequence target* 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 and described below:

- Each of the DBAs and any high-consequence DECs are examined to determine which plant equipment are available to perform the risk-significant *required safety functions*. Then, one or more of available plant equipment are selected to perform each safety function that covers all the DBAs and high-consequence DECs.
- The minimum set of specific plant equipment that can be solely relied on during DBAs are classified as *safety systems* and considered in the conservative deterministic safety analysis of the DBAs.

- The remaining plant equipment are further evaluated for their risk-significance to determine if their safety function is necessary to keep the risk from one or more event sequences within the frequency-consequence target or if it makes a significant contribution 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* as an item or process that is designed to perform a safety function, or that 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, it is classified as a *safety related item*.
- The plant equipment that are neither safety- nor risk-significant are further evaluated to determine if they play a role in ensuring DiD adequacy as discussed in the last step. If not, they are considered as *items not important to safety*.

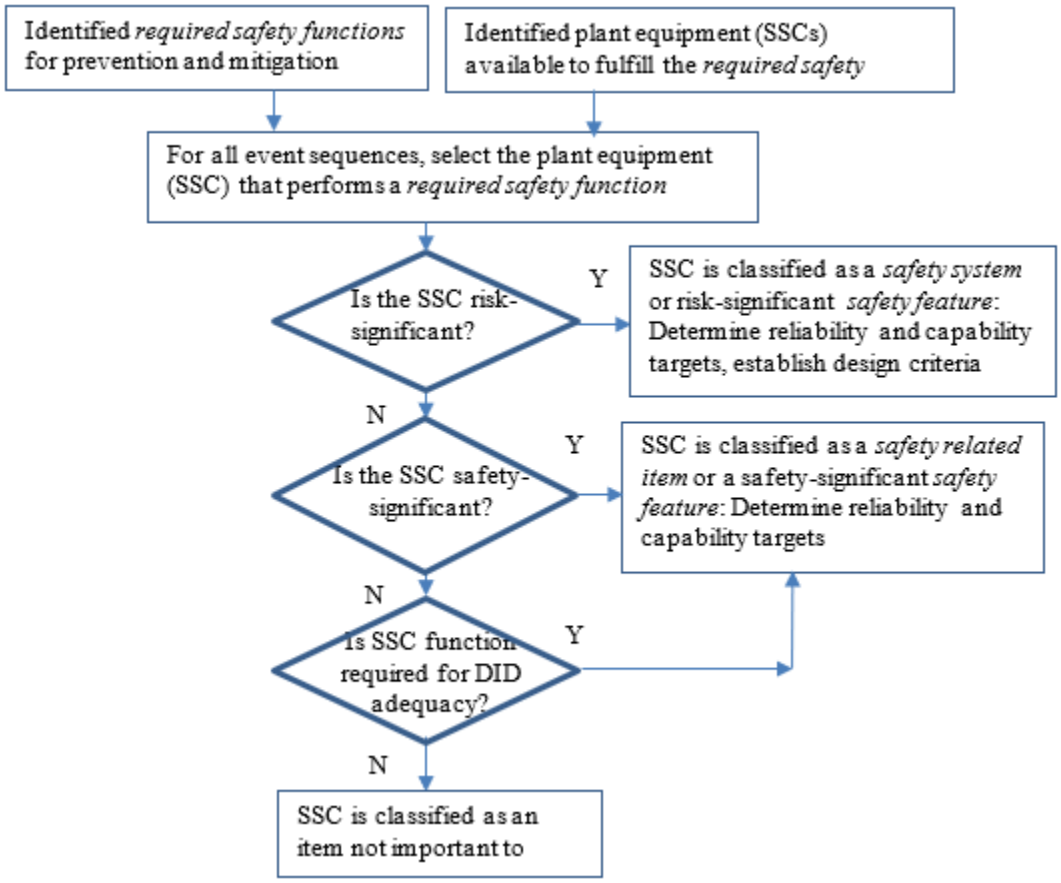

Figure 5. Plant equipment (SSC) safety classification process.

Finally, 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.

Deterministic Safety Analyses

This step 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 defense 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 as shown in Table 3 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 conservative deterministic safety analysis.
- 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 deterministic 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.

Evaluation of Defense-in-Depth Adequacy

The main goal of this step is to ensure that all *required safety functions* are achieved with sufficient margins to compensate for the uncertainties. The evaluation 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 first four levels of DiD include reliance on at least two (ideally three) independent 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.

DiD is deemed to be adequate when:

- DiD guidelines to achieve the design goals listed in Table 4 are satisfied,
- Risk margins against frequency-consequence target are sufficient and cumulative risk targets are met,
- Role of plant equipment in prevention and mitigation at each layer of defense is understood and prevention-mitigation balance is achieved without excessive reliance on one vs. the other,
- Independence of design features at each layer of defense is sufficient, 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, 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.

Table 4. 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 this level.
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*. The event sequences that would lead to an unacceptably early or large radioactive release are required to be 'practically eliminated' by implementing design provisions.

Decision on Completion of Design Development

A decision is made if additional design development is warranted, 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 4. When the list of initiating events and associated event sequences are finalized, it will likely lead to a more robust design with more adaptive defense measures based on safety-by-design principles than what could be achieved with via deterministic considerations alone.

REFERENCES

1. 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).
2. "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.
3. Task Force on Safety Design Criteria, Generation IV International Forum (GIF), https://www.gen-4.org/gif/jcms/c_93020/safety-design-criteria