A Risk Informed Defense-in-Depth Framework For Existing and Advanced Reactors

By

Karl N. Fleming[1] and Fred A. Silady
Technology Insights
6540 Lusk Blvd., Suite C-102
San Diego, CA 92121-2767, USA

Abstract

The philosophy known as "defense-in-depth" has been used extensively in nuclear reactor safety evaluations and in justifying regulatory decisions. An evolving number of definitions of this philosophy have been proposed, primarily from a regulatory perspective. The purpose of this paper is to review the current definitions of defense-in-depth and to offer solutions to the technical issues identified from this review. A more general definition of defense-in-depth is proposed that can be used for any reactor concept. The proposed definition includes an explicit consideration of how the inherent characteristics of the reactor set the foundation for the safety case, an examination of how design features of a reactor employ the strategies of accident prevention and mitigation, and how to quantify the importance of design features responsible for prevention and mitigation. Application of this approach is demonstrated with use of examples for Pressurized Water Reactors (PWRs) and Modular High-Temperature Gas-Cooled Reactors (MHTGRs).

KEY WORDS: Defense-in-depth, prevention, mitigation, probabilistic risk assessment, advanced reactors, safety functions, LWR, MHTGR, PBMR

INTRODUCTION

A nuclear power reactor can be described in terms of its inherent reactor characteristics, and a set of engineered systems, structures and components (SSCs) that perform various power production and safety functions. The defense-in-depth philosophy, as it has been applied to currently operating reactors, dictates that the engineered SSCs include a set of radionuclide transport barriers and engineered safety features to protect the integrity of these barriers. It is useful in this discussion to distinguish between those features that are inherent to the application, e.g. to generate electrical power, and those that are provided for the primary purpose of performing safety functions.

The inherent characteristics of a reactor are defined here as the properties of the materials selected for the fuel elements, fuel cladding, moderator (in the case of a thermal reactor), the coolant or working fluid, and other design parameters that are dictated by the intended application. The light water reactor concept used in most

[1] Corresponding author: flemıng@tı-sd com

currently operating plants, the PWR, was originally developed for the U.S. Navy in response to their need for a shipboard power plant having a relatively high power density that could propel submarines for long periods of time submerged. (See any textbook on Nuclear Engineering such as [1]). These requirements constrained the design of the core, the power density, the selection of moderator and coolant, fuel enrichment, and other design parameters. With the benefit of large investments in the materials technology for these early military reactors, the early Naval reactor designs were subsequently modified and adapted to civilian power production applications as part of a government energy policy known as "Atoms for Peace". The U.S. Navy's role in the design of the LWR is evidenced by the fact that the first commercial nuclear power plant at Shippingport was designed under a team led by Admiral Rickover and operated by the U.S. Naval Reactors [1].

While there were many changes in the LWR designs necessitated by their use in civilian energy production, such as improvements to the fuel and introduction of a reactor containment, the inherent features of the LWR developed for nuclear submarines are essentially the same as those for current LWRs used for stationary, civilian power plants. There are of course exceptions such as the introduction of boric acid into the light water coolant/moderator in the PWR and the change to a low enriched fuel which changed some of the core characteristics. As more plants were licensed and insights from operating experience including several incidents and accidents were developed, the defense-in-depth concept evolved. This evolution maintained the fundamental elements of defense-in-depth such as the use of multiple barriers to radionuclide transport including the fuel, coolant pressure boundary, and containment, and the introduction of engineered safety features to perform a set of safety functions whose ultimate objective is to protect the integrity of these barriers.

While the inherent features of the LWRs play an important role in definition of safety functions and help define the design parameters of the engineered safety features, their role in the definitions of defense-in-depth has been largely obscured. That is evidenced by the preoccupation with engineered safety features in the available definitions of defense-in-depth at the expense of the inherent features. This was not an issue while licensing a fleet of plants with the same inherent features, but it becomes an issue when considering defense-in-depth strategies for the design and licensing of reactors with fundamentally different inherent features, such as graphite moderated, helium cooled, and particle fuel reactors, for example.

Current generation light water reactors were designed, built, and licensed using a deterministic approach to evaluating safety. This approach included the definition of design basis accidents and general design criteria including requirements that certain engineered safety features be provided to mitigate these accidents. To reduce the likelihood of experiencing conditions outside the design basis envelope, a single failure criterion was adopted which forced a minimum level of redundancy of safety systems and, in selected instances, requirements for some diversity were also included. The requirements called for containment structures and associated engineered safety features to be conservatively designed to protect the public in response to these design basis events. The early definitions of defense-in-depth were framed in the context of this deterministic safety philosophy.

The early emphasis of safety features for LWRs was to provide reliable means of reactivity control including negative temperature coefficient of reactivity and so-called "fail safe" design features for the reactor trip systems. The emphasis on decay heat removal considerations came later and was introduced only after the first prototypes were built. Indeed, a number of early plants such as Indian Point Unit 1 and Dresden 1 were built with no emergency core cooling systems or onsite emergency AC power systems as required in present day reactors [2]. It was not until the licensing of Dresden 2 and Indian Point 2 that the capability of containments and associated engineered safeguards to cope with severe core melt accidents was considered and reviewed in some detail [2]. Containment considerations evolved from an original function of providing a "vapor container", to collect leakage of contaminated primary coolant, but with limited structural capabilities. Later containment requirements were enhanced to provide protection against external missiles, however, none of the containments on existing U.S. plants were specifically designed to contain a severe core damage accident. That is to say, core damage events, and the associated loads imposed by various severe accident phenomena remain to this day outside the design basis accident envelope. Design basis loads for the containment structures were conservatively defined but under the assumption that severe core damage would be prevented. Subsequently, it was determined in PRAs and severe accident research programs that conservatisms and safety margins that were employed to design the containments to withstand the loads from the design basis accidents resulted in a significant capability of the containments to mitigate the consequences of core damage accidents, although the extent of protection was determined to vary widely among reactor and containment types. This insight validated at least certain aspects of the defense-in-depth philosophy, including the prudent application of conservative safety margins to protect against the design basis accidents.

As more plants were built and more service experience acquired, new rules were progressively added yielding a very complex set of requirements for the last part of the existing fleet of reactors to be built [2]. During the licensing of the current fleet of plants and the accumulation of experience with various incidents and accidents, a growing list of unresolved safety issues emerged. The most notable of these incidents and accidents were the Browns Ferry fire and the TMI-2 accident. Many additional incidents occurred, including literally hundreds of common cause failures in redundant safety systems. This experience casts doubt on the wisdom of excluding common cause failures from the design basis envelope, thereby exposing a serious limitation of the single failure criterion as a tool to help define what is credible. More recently, the vessel head degradation at Davis-Besse exposed a susceptibility of the coolant pressure boundary to a damage mechanism that is inherent to the properties of the vessel materials and in the presence of boric acid in the primary coolant.

From the authors' perspective, these events raise questions about the adequacy and sufficiency of the deterministic approach to safety as well as challenge the completeness of the PRAs. The same uncertainties that are exposed in the course of attempting to perform a PRA are available to challenge many of the decisions that are made in the deterministic approach, especially those that involve deciding on what is to be deemed "credible" or what level of safety margin is to be considered "adequate". In fact, lessons learned from reactor operating experience helped build the impetus towards a more risk informed approach to safety assessment. Unfortunately, these experiences also led to a need to keep redefining the defense-in-depth concept, as the extent of the defenses that were needed could not be fully determined a-priori.

The defense-in-depth concept that we know today is not what was used to develop the current reactor concepts. Rather, it has evolved to reflect the collective knowledge that has been acquired over the course of building the first 100 or so plants and experiencing a large fraction of their design lifetimes. The lessons from a number of serious incidents and accidents, and more than three decades experience with performing and applying PRA has greatly contributed to this knowledge base. A real question is whether these lessons have been adequately reflected in the current definitions of defense-in-depth.

Definitions of Defense-in-Depth

An insightful discussion of the evolution of thinking about defense-in-depth from the perspective of the USNRC Advisory Committee on Reactor Safeguards is provided in Reference [3]. The authors of this reference characterize the divergence of views on how to define defense-in-depth into two camps: The "structuralist" school advances the notion that defense-in-depth is embodied in the regulations and in the design of facilities that are built to comply with the regulations. The "rationalist" school asserts that defense-in-depth is the set of provisions that are made to compensate for uncertainty and incompleteness in our understanding of accident initiation and progression that largely result from the application of Probabilistic Risk Assessment methods to determine whether quantitative safety goals have been met. Attempts to balance, integrate, and "blend" the concepts from these two schools of thought have inspired the current movement towards a more risk informed, albeit deterministic regulatory process. The need for this regulatory reform appears to be the realization that the "structuralist" viewpoint of defense-in-depth had created an imbalance in the application of resources within the design basis envelope at the expense of the risk management of severe accidents that exceed that envelope.

A summary of selected definitions of defense-in-depth is provided in Table 1 and include those developed by respected regulatory bodies over the years[2]. As seen in the table, the definitions have evolved from a rather simple set of strategies to apply multiple lines of defense to a more comprehensive set of cornerstones, strategies, and

[2] In the peer review of an earlier draft of this paper it was pointed out that the regulations governing nuclear power include one definition of defense-in-depth in 10 CFR Part 50 Appendix R which sets rules for fire protection in older plants. This definition sets forth the following objectives for the defense-in-depth of fire protection: Prevent fires from starting, detect rapidly, control and extinguish the fires that do occur, and to protect SSCs needed to safely shutdown the plant from the effects of the fire and fire fighting activities.

tactics to protect the public health and safety. The latest definitions have become rather broad and inclusive as they touch on practically all aspects of design, operation, site selection, and regulation of nuclear power. This breadth in scope of the definitions has advantages in that it provides a more complete explanation of the concepts of defense-in-depth. However, the inclusive nature of the explanation lacks focus and thereby makes it less predictable in how it will be invoked in future regulatory decisions.

Imbedded in these definitions are three distinct usages of the term defense-in-depth. The first of these and probably the most clearly understood refers to a set of well defined design features in a nuclear power plant that provide multiple and physical lines of defense between the hazard and the public. The hazard is an inventory of radioactive material and the potential for the release of such material to the environment that could harm the health or safety of the public. These lines of defense include multiple radionuclide transport barriers and engineered safety features to perform safety functions which support the integrity of these barriers. The transport barriers include physical barriers that prevent or block the movement of radionuclides and time delays in the movement that allow for the radioactive decay and deposition of nuclides prior to their release. The authors refer to this usage of the term as ***design defense-in-depth.***

There is a second usage of defense-in-depth that is especially implied in the “structuralist” definition referred to in Reference [3] that incorporates defense-in-depth thinking into the licensing requirements. These requirements include the single failure criterion, safety margins reflected in various acceptance criteria, special treatment requirements, and the General Design Criteria. Although there is relationship between these requirements and the detailed design features that are reflected in ***design defense-in-depth,*** they are not one in the same as they are controlled by different stakeholders in the process. The authors will henceforth refer to this usage of the term as ***process defense-in-depth.***

There is a third usage of the term defense-in-depth that is especially dominant in the IAEA version in which the concept is defined in terms of a scenario framework. This perspective includes initiating events, strategies to prevent initiating events from occurring and from progressing to accidents, and strategies to mitigate the consequences of events and accidents. The authors refer to this usage of the term as ***scenario defense-in-depth.*** This type of defense-in-depth reflects the PRA perspective of safety philosophy in which all conceivable combinations of initiating events and successes and failures of plant safety features are considered in the definition of scenarios.

Table 1 Review of Selected Definitions of Defense-in-Depth

Author	NRC(AEC)	NRC	IAEA	NRC	NRC
Date	1967	1994	1996	1998	2000
Reference	[4]	[6]	[7], [8], [9]	Reg. Guide 1.174 [10]	[11]
Key Elements of Proposed Definition	1. Prevention of initiating events 2. Engineered safety features to prevent accidents 3. Consequence limiting systems to prevent large releases	1. Prevention of initiating events 2) Safety systems to prevent accidents 3) Containment to limit releases 4) Accident management 5) Reactor siting and emergency planning	1. Prevention of abnormal operation and failures 2. Control abnormal operation and detection of failures 3. Control accidents within design basis using ESF and procedures 4. Control of severe conditions by preventing accident progression, mitigation by accident management 5. Mitigation of radiological consequences via emergency response	1. Balance between prevention and mitigation 2. No over-reliance on programmatic activities to compensate for weaknesses in plant design 3. System redundancy, independence, and diversity 4. Potential common cause failures are minimize through the use of passive, and diverse active systems to support key safety functions 5. Barriers to radionuclide release are independent, and 6. The potential for human errors is minimized.	Reactor Safety Cornerstones • Prevent initiating events • Mitigation systems • Barrier Integrity • Emergency preparedness Accident Prevention Strategies 1. limit frequency of initiating events 2. limit probability of core damage given initiating event Accident Mitigation Strategies 3. limit releases given core damage 4. limit public health effects given release Tactics to implement strategies: • Safety margins • Redundancy, diversity, independence • General design criteria • Special treatment, etc.

Incorporation of Risk Insights into Defense-in-Depth

It is important to note that the need to incorporate risk insights into the definitions of defense-in-depth stemmed in part from the weaknesses in the deterministic approach to safety philosophy that were exposed by PRA insights as well as by some of the most important incidents and accidents. These insights include:

- Risk dominated by events beyond design basis. The risk to public health and safety from operation of LWR nuclear power plants is dominated by the risks from severe core damage accidents that are beyond the design basis; the design basis accidents are not risk significant in part because they must have negligible consequences to meet the design basis accident consequence criteria.
- Events beyond the design basis not always rare. A presumption of the deterministic approach to safety is that if all the requirements are met, accidents more severe than the design basis accidents are so infrequent as to be incredible. However this is directly contradicted by the first insight. Risks from severe core damage accidents are in turn dominated by multiple dependent failures including external events, internal fires and floods, common cause failures and human errors that have little respect for the single failure criterion. In fact, there is a body of evidence from completed PRAs that suggests that some beyond design basis core damage accidents are even more likely than the so-called limiting design basis accidents. For example the CDF estimates in current LWR PRAs, whose mean values are in the range of $1x10^{-6}$ per year to more than $1x10^{-4}$ per year, yield much higher frequencies than any reasonable estimate for a typical design basis LOCA scenario that includes a double-ended pipe break, concurrent loss of offsite power, followed by failure of the limiting train of safety related systems. This insight exposes the uncertainties that are inherent in any attempt to characterize the likelihood of rare events. These uncertainties are reflected in PRAs by preventing the accurate estimation of rare accident frequencies. These same uncertainties are dealt with in the deterministic application of defense-in-depth in the form of unverified, qualitative judgments about whether events are to be deemed credible or whether existing safeguards provide adequate protection.
- Radionuclide barriers are not independent. The goal of barrier independence used in the defense-in-depth definition in RG 1.174 implies that the probability of failure of each barrier does not significantly increase given failure of another barrier. The risk dominant core damage accidents identified in the LWR PRAs reveal numerous examples in which dependent failures of multiple radionuclide barriers are postulated to occur, violating the principle of independent radionuclide barriers. Interfacing system LOCAs[3], and numerous interactions between failure modes of the core, coolant boundary, and containment that are evident in the all the PRA results are

[3] These are failures at interfaces between the reactor coolant system and interfacing systems such as the ECCS systems that result in a loss of coolant outside the containment bypassing the ECCS sumps and resulting in a release pathway from the reactor coolant system to the environment, bypassing the containment. As analyzed in PRAs these scenarios are typically assumed to result in core damage and large early release.

examples of this. When the conditions necessary for core damage are reached the effectiveness of the coolant boundary to retain any radionuclides that are released from the damaged core into the coolant stream is lost. Furthermore, unless the primary coolant system is at pressure equilibrium with the containment at the time of release from the fuel, any of those releases will be driven from the coolant system though one or more of the openings that are inevitable in any particular core damage scenario. Depending on the initiating event and accident sequence, release of circulating coolant activity from the boundary is certain to occur given core damage from one or more of the following: breach of the boundary as a LOCA-type initiating event, lifting of the coolant relief valves into the containment, or consequential failure of the vessel and/or pressure boundary due to severe accident loadings. During the TMI-2 accident, a large fraction of the core inventory of noble gases, halogens, and Cesium isotopes were released from the fuel into the coolant and into the containment, however the core cooling functions were restored in time to prevent the migration of core debris from the pressure boundary[4]. Furthermore, radionuclides that were not released into the containment, such as essentially all the actinides and non-volatile species, resulted from properties of the fuel and not the retention capabilities of the pressure boundary as these radionuclides were retained in the intact and damaged fuel rods. Hence, the conditional probability of loss of the reactor coolant pressure boundary as a barrier to radionuclide released from the fuel given core damage approaches unity, resulting in a heavy reliance on the containment to enforce the barrier defense-in-depth principle for scenarios involving core damage. For this reason it is misleading to list the fuel and the coolant pressure boundary as separate and independent barriers in the context of barrier defense-in-depth.

- <u>Containments mitigate some events beyond design basis.</u> Even though the containment structures in the current fleet of plants were not specifically designed to contain the releases and severe accident phenomenological loads from a severe core damage event, conservatisms included to protect against design basis loss of coolant accidents were found to result in a significant capability to protect against severe accidents in PRA evaluations. This capability varies among reactor and containment designs and is especially significant for those with large containment volume to thermal power ratios.
- <u>Containments are rarely an independent barrier.</u> While the containment plays an important role in protecting against a severe core damage event, the results of PRAs clearly show that the goal of barrier independence with this feature has not been achieved. The risk metric available to measure this property is the conditional

[4] According to Reference [12], based on measurements that were made after the accident, the distribution of the Cs and I isotopes at the end of the accident were as follows: 30% in intact fuel rods, 10% in damaged fuel rods and core debris, 47% in the reactor building, 5% bypassed into the auxiliary building, and 3% retained in the RCS pressure boundary outside of the vessel. (Only 95% of the inventory was accounted for in these measurements). For the noble gases essentially all that was not retained in the fuel was released to the containment. A large fraction of the less volatile nuclides were retained in the intact and damaged fuel rods and debris. Hence the RCS pressure boundary provided very little retention for any of the isotopes that were not retained by the fuel.

probability of containment failure given core damage (CCDP). Insights from PRAs have shown that this metric is dominated by dependent failure mechanisms such as interfacing system LOCAs, other containment bypass sequences such as SG tube ruptures, and sequences in which a severe accident process imposes loads on the containment that exceed its capacity. These loads cover a wide set of core-coolant-containment interactions that are not consistent with barrier independence. An important insight from PRAs is that the conditional containment failure probability is highly variable and approaches unity for containment bypass sequences. The potential for containment bypass stems from a lack of concentric barriers, i.e., situations in which the part of the reactor coolant pressure boundary could fail and create a release path that bypasses the containment. Unless the barriers are concentric, they cannot be independent. Hence, even though for most situations the CCDP for current reactors is less than unity, they are much higher than they would be if the dominant containment failure modes were independent of the core damage modes. Hence to say that the containment barrier has achieved independence in relation to the coupled fuel/pressure boundary barriers would be a gross overstatement. The only failure mode considered in current PRAs that can be argued to be reasonably independent of the fuel barrier is failure to close any pre-opened containment isolation valves, and these failure modes only rarely surface in the list of important risk contributors. Hence, for all practical purposes, the containment failure probability is dominated by modes that are highly dependent on core damage modes, and hence cannot be regarded as an independent barrier. However there is indeed less dependence than between the fuel and coolant boundary failure modes.

- Common cause failures important for redundant active systems. Accident sequences involving failures of redundant active systems are dominated by common cause failures. This insight is corroborated by service experience which has shown several examples of redundant system failures due to these causes.

The above perspectives indicate both strengths and weaknesses to the deterministic model for defense-in-depth. While insights from TMI-2, other service experience, and PRAs have taught us that events beyond the design basis are not as unlikely as once believed, defense-in-depth thinking in setting the requirements for the design basis accidents resulted in margins in the containment designs that prevented significant releases at TMI-2 and are expected to mitigate even more severe core damage events based on the results of PRAs.

Critique of Current Definitions

The most recent definition of defense-in-depth, the last column in Table 1, that is being used by the NRC as part of their effort to risk inform the LWR General Design Criteria [11], incorporates key insights from LWR PRAs: namely that the risk of an LWR can be managed by strategies to reduce the core damage frequency and to limit the releases from core damage accidents. What is not mentioned (and not in the scope of the document) is the extent to which this insight is specific to the characteristics of the LWRs and how it can be applied to reactors with characteristics that are fundamentally different than LWRs. There is quite a lot of "baggage" that comes with the definition of core damage states for the LWRs that is derived from its inherent reactor characteristics which may or may not apply to advanced reactor concepts. While reactors such as the PBMR and MHTGR have various damage states that can be associated with a set of defined consequences, there is no single core damage state that forms a natural pinch point for localizing all risk significant accident sequences as is the case with LWRs.

The risk-informed framework for defining defense-in-depth in Reference [11] is regarded by the authors as an improvement over its deterministic predecessors and should provide a useful purpose in guiding the efforts to reform the regulatory process for current generation LWRs. While this framework seems quite reasonable for its stated purpose for the existing LWR designs, it has several limitations for examining how defense-in-depth has been employed in advanced reactors, particularly those with characteristics fundamentally different than LWRs. These limitations include the following:

- Important risk insights identified in the previous section have not been incorporated into the available definitions, particularly those regarding barrier dependence, the clarification of the meaning of prevention and mitigation, and the fact that the proposed balance between prevention and mitigation does not exist.
- The role of the inherent features of the reactor, including the selection of materials and design features of the core, fuel elements, moderator, and reactor coolant, in contributing to defense-in-depth is not explicitly delineated. The inherent features of a reactor help define the success criteria for terminating event sequences, which in turn define the reactor specific safety functions that are needed to protect the barriers. In addition, the inherent features govern the various accident phenomena that help determine accident consequences and associated mitigation strategies. As a result, the importance of inherent features in supporting the defense-in-depth concept has been obscured. Consequently, the importance of engineered features, is greatly overstated. Due to the fact that defense-in-depth was introduced after the inherent features of the LWR were established, this is understandable. However, to determine how well defense-in-depth philosophy is incorporated into advanced reactor designs, an understanding of the role of the inherent features is essential[5].
- Risk metrics that are tied to a reactor specific definition of core damage such as CDF are not fundamental to reactors in general safety but rather are tied directly to definitions of reactor specific core damage states. LWR success criteria to avoid core damage such as specified by minimum reactor vessel coolant levels, peak core

[5] The importance of inherent safety features in defining the regulatory requirements for advanced reactors is not a new idea. See for example, References [13] and [14].

temperatures, etc. are tied to the inherent characteristics of the fuel, the fuel element cladding and reactor coolant. For example, the fuel temperature in an LWR that would produce severe metal water reactions is significantly less than normal operating fuel temperatures in a PBMR or MHTGR. The appropriate safety functions and scenario end states for each reactor need to be developed in light of its inherent characteristics. These end states may or may not be analogous to core damage in an LWR, depending on the inherent features. In addition the relative importance and significance of each barrier in the respective defense-in-depth approach may indeed be different.

- The concept of balancing the strategies of accident prevention and accident mitigation, though intuitively appealing, has not been clearly defined or justified. If one replaced a design feature for mitigating accidents in a reactor having balanced strategies with something that is more robust, the balance would be upset but the safety would be enhanced. Hence, the most balanced designs are not necessarily the ones that present the lowest risk, or the most faithful to the defense-in-depth philosophy. Also for a given reactor design, the degree of so-called balance between the prevention and mitigation will vary from sequence to sequence. From a risk management perspective, higher frequency sequences tend to rely more heavily on mitigation, whereas lower frequency sequences tend to rely more on prevention, as will be demonstrated below using several examples for two different reactor types.
- What is meant by prevention and mitigation needs to be defined more clearly to be useful in designing, constructing, and operating the next generation of reactors. A given design feature may provide both preventative and mitigative functions across the sequences in a PRA model. Also, there is no unique point of reference from which to perceive prevention and mitigation. One can prevent or mitigate initiating events, any conceivable plant state, or any pinch point along an accident sequence. The selection of an event sequence pinch point to discuss prevention and mitigation is arbitrary. This conclusion is evident in the available NRC definitions of defense-in-depth. The Appendix R definition uses the occurrence of a fire along the sequence for the balance point in defining defense-in-depth for fire protection, whereas the risk informed Appendix B definition uses the point of core damage. This lack of unique reference point makes it pointless to argue whether prevention and mitigation can be balanced.
- The current LWR framework for defense-in-depth reflected in [11] does not explicitly address expectations for enhanced, passive, and inherently reliable safety features reflected in NRC's Advanced Reactor Policy [14]. That policy encourages a shifting from dependence on engineered safety systems with active components towards inherent safety and the capability to perform the necessary safety functions with passive and inherently reliable means. It is not clear that it is either possible or desirable to maintain the so-called balance between prevention and mitigation as the designs rely on more passive and inherent features.
- The all inclusive breadth of the most recent risk-informed definitions could use some organization to identify the roles of designers, operators, and regulators in implementing the defense-in-depth strategies.

DEFENSE-IN-DEPTH FRAMEWORK FOR ADVANCED REACTORS

While the defense-in-depth concept has served the regulatory decision making process well, the previous sections of this paper have identified several reasons to revise its definition to gain the most benefit from it in the design and licensing of advanced reactor concepts such as the high temperature reactors. These reactor concepts are cited as they exhibit fundamental differences in the inherent features compared with the reactors that were used to advance the defense-in-depth concept. Many of these differences are discussed in Reference [15].

The authors propose an alternative definition of defense-in-depth that is comprised of the following major elements:

- ***Design Defense—In-Depth***
- ***Process Defense-In-Depth***
- ***Scenario Defense-In-Depth***

Design Defense-in-Depth reflects all the decisions made by the designer to incorporate the defense-in-depth into the physical plant.

Process Defense-in-Depth reflects all the decision made in the formulation of regulatory requirements associated with licensing, operating, maintaining, and inspecting the plant and in all the processes that contribute to safety. These processes cover the design, construction, operation, maintenance, testing, and inspections that ensure safe operation of the facility.

Scenario Defense-in-Depth reflects the development and evaluation of strategies to manage the risks of accidents, including the strategies of accident prevention and mitigation. This aspect of defense-in-depth also provides the framework for performing the deterministic and probabilistic safety evaluations which help determine how well various prevention and mitigation strategies have been implemented.

In support of each of these elements of defense-in-depth is a comprehensive PRA which helps to ensure that all decision making in these processes is properly evaluated and risk-informed. For example, information needed to implement ***Scenario Defense-in-Depth*** is provided by a comprehensive plant specific PRA that is developed and maintained to support the entire life cycle of decisions that bear on the safe operation of the plant.

The breakdown of defense-in-depth into different categories is done to support the different types of decisions that are needed to implement a comprehensive strategy for safe plant operation throughout its lifetime. The components and relationships among these elements of the proposed comprehensive defense-in-depth framework are explained in the following:

Design Defense-in-Depth

Design Defense-in-Depth reflects the high level safety philosophy for the use of multiple lines of defense in the design of the plant safety features. This includes the selection of the plant site in relation to the surrounding population, the selection of the inherent features of the reactor that dictate its fundamental behavior during normal, abnormal and accident conditions, the design of barriers between the radionuclide sources and the environment, and the design of engineered safety features to support an appropriate set of safety functions that support the integrity of these barriers.

A rather fundamental starting point for many of the historical definitions of defense-in-depth is the concept of barrier defense-in-depth as conceptualized in Figure 1. In this concept, a set of multiple physical barriers is introduced between the hazard, the inventory of radioactive material in the reactor, and the environment. A model for these barriers that seems to cover all the existing and advanced reactors under discussion consists of the fuel element and its cladding, a reactor coolant system pressure boundary, and containment or confinement representing the last barrier to an environmental release. Provisions for reactor siting at a distance in relation to the surrounding population is also included as a fourth "barrier" as illustrated in the figure. In contrast with current LWR designs, the barriers are all shown in the figure as being concentric which embodies the most independent configuration that can be postulated.

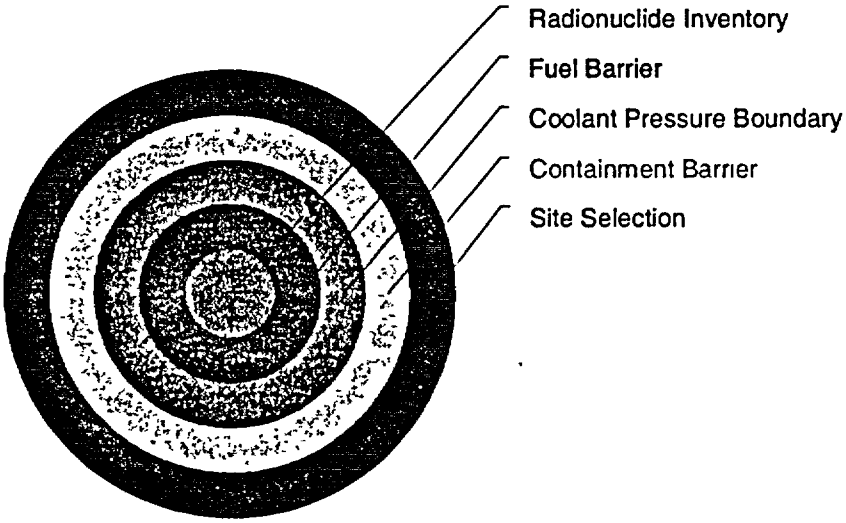


Figure 1 Elements of Barriers In Defense-in-Depth

Important attributes of the barrier defense-in-depth concept are to ensure that the barriers are concentric as one strategy to make them independent. An important insight from PRAs addressed previously is the fact that when these barriers are not fully concentric, risk significant accident sequences associated with containment bypass may result. Another insight is that the extent to which independence between the barriers can be assured is largely determined by the interactions between the inherent characteristics of the reactors and the barriers themselves during potential accident sequences. The barrier defense-in-depth concept is most effective when the barriers are concentric and when postulated failure modes of one barrier do not lead to the likely failure of another barrier or to significant increases in the probability of failure of the barrier. Again this ideal achievement of barrier independence has not been demonstrated or even plausibly argued for the existing reactor concepts.

Design Defense-In-Depth is comprised of radionuclide transport barriers including the fuel barrier, the coolant pressure boundary, and containment, as well as design strategies to ensure the integrity, effectiveness, and hence, a minimized dependence of these barriers, as illustrated in Figure 2. The safety design approach utilizes the inherent features and characteristics of the reactor defined by the selection of materials and basic design aspects of the reactor core and associated fuel elements, the selection of materials and basic design aspects of the moderator (in the case of advanced thermal reactors) and the selection of the reactor coolant. These reactor characteristics are inherent to the reactor concept and provide the foundation for the safety case either directly by contributing to the integrity of the radionuclide barriers or by dictating the requirements for engineered safety features that are provided to support barrier integrity, or a combination of these. Such features also dictate the time available to implement emergency measures such as accident management and offsite protective actions. No matter what the reactor concept is, its overall safety is determined by the combination of inherent and engineered safety features and how these features interact to prevent and to mitigate accidents that may challenge the integrity of the three primary barriers to radionuclide release. As noted earlier, strategies to ensure independence of the barriers are consistent with making the barriers concentric.

Once the inherent safety features are defined, the safety functions that must be satisfied to achieve safe sequence end states and to protect the radionuclide barriers can be determined. Different inherent features of the reactors will necessarily lead to different minimum sets of safety functions that need to be supported to protect the barriers. For example coolant inventory control is an essential safety function for light water reactors as failure to control inventory would lead to core damage and large releases from the fuel unless such inventory loss is not replaced. By contrast for many gas-cooled reactors such as the PBMR and MHTGR, coolant inventory control although necessary to produce electric power is not relevant to protecting the integrity of the fuel. The only truly fundamental safety functions are those necessary and sufficient to protect the radionuclide transport barriers. The specific safety function required to accomplish this are reactor specific and determined by the properties of the inherent features.

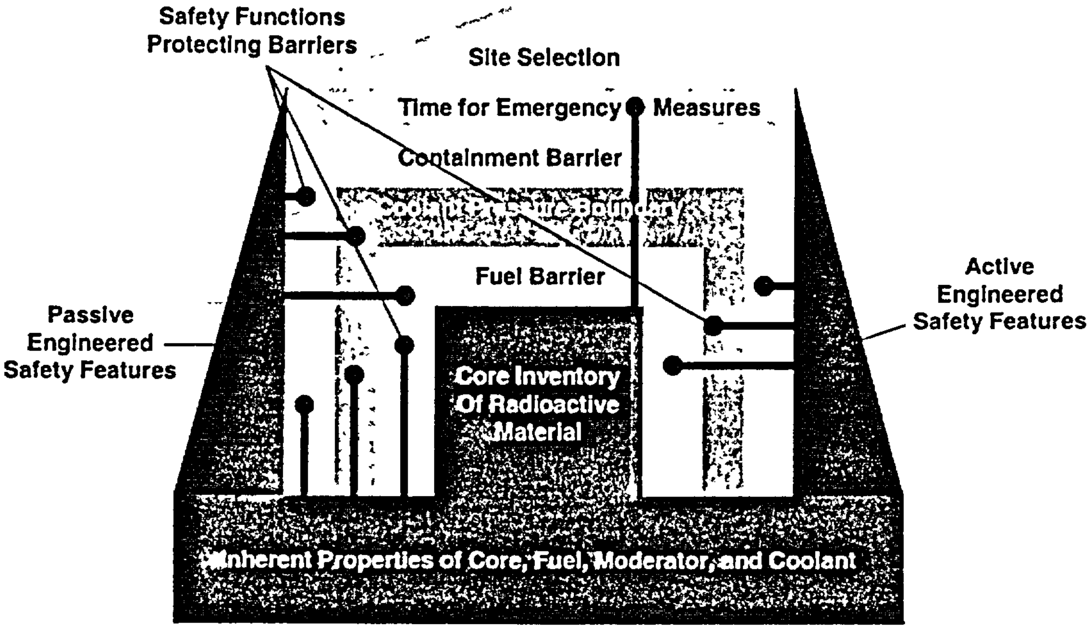


Figure 2 Elements of Design Defense-in-Depth

In the design of the engineered safety features to support each safety function there are both passive and active strategies to consider. It is generally accepted that passive safety features such as negative temperature coefficient of reactivity and passive means of heat removal are inherently more reliable than systems requiring the operation of active components so long as the material condition of the components and structures that perform the passive functions are adequately maintained. The need and importance of any engineered active features is evident once the inherent and engineered passive features are understood.

So, in summary ***Design Defense-In-Depth*** is comprised of the use of multiple barriers between the radioactivity hazard and the environment, and design strategies to ensure the integrity of the barriers under normal and accident conditions. These design strategies include the selection of inherent features, the use of concentric and independent barriers, and additional engineered safety features to provide each reactor specific safety function. Engineered safety features include passive features including the barriers themselves and, where appropriate, additional active safety systems to support the integrity of the barriers. It is important to note the explicit representation of the inherent safety features of the reactor for those features provide the foundation for the design of the barriers, dictate what safety functions must be provided to support these barriers, and dictate options available to use passive rather than active safety systems to support these functions. This characterization addresses a deficiency noted in the previous definitions of defense-in-depth and makes it possible, at least in principle, to compare different defense in depth strategies among reactors with inherently different characteristics. The major elements of ***Design Defense-in-Depth*** are listed in Table 2. The major improvements to this aspect of defense-in-depth as viewed by the authors include the explicit consideration of inherent features which help define reactor specific safety functions and the delineation of engineered safety functions into those that employ active and passive systems.

Table 2 Elements of *Design Defense-in-Depth*

- Inherent features of reactor important to safety
  - Fundamental properties of core/fuel elements
  - Fundamental properties of reactor coolant
  - Fundamental properties of moderator (thermal reactors only)
- Use of multiple barriers
  - Fuel barrier design features
  - Coolant pressure boundary design features
  - Containment design features
  - Independence and concentricity of barriers
- Engineered safety features to protect barrier integrity
  - Reactor specific safety functions to protect barriers
  - Passive engineered safety systems
  - Active engineered safety systems
  - Operator actions needed to implement or inhibit safety functions
- Detailed design decisions to ensure adequate reliability of barriers and engineered safety features meeting requirements set in ***Process Defense-In-Depth***
- Selection of appropriate reactor sites
- Time available to implement emergency measures

Process Defense-in-Depth

Process Defense-in-Depth sets requirements and criteria for all decisions that are made in the life cycle of the plant that contribute to plant safety. These decisions include those involved in the design, licensing, operation, maintenance, training, and oversight of operation. Process defense-in-depth activities and associated controls provide assurance that the barriers and other safety features are in good material condition and will operate with adequate safety margins for all envisioned normal, upset and accident conditions in a manner that will meet all relevant top level regulatory requirements for the plant lifetime. These activities and controls include technical specifications, special treatment requirements, criteria to establish adequate plant and equipment performance, in-service testing and inspection, operator training, emergency operating procedures, severe accident management guidelines, management oversight, and emergency planning. The key elements of ***Process Defense-in-Depth*** are listed in Table 3. The basis for the specific requirements is derived from ***Scenario Defense-in-Depth***, as described below.

Table 3 Elements of *Process Defense-in-Depth*

- Regulatory requirements
  - Top Level Regulatory requirements (TLRC, e.g. safety goals)
  - Selection of Licensing Basis Events
  - Classification of Safety related SSCs
  - Definition of safety margins for deterministic safety evaluations
  - Special treatment requirements
  - Design reviews
- Organizational and Human Factors
  - Management safety culture
  - Operator Training requirements
  - Emergency Operating Procedures
  - Accident management guidelines
- Technical Specifications
  - Limited Conditions for Operation
  - Surveillance testing requirements
  - Allowable outage (Completion) times
- Maintenance and Monitoring of SSC Performance
  - Startup testing
  - Fuel manufacturing tests and inspections
  - In-service testing
  - In-service inspection
  - Maintenance of SSCs
  - Selection of appropriate performance indicators
  - Regulatory inspections and oversight
  - Corrective action programs

Scenario Defense-in-Depth

Scenario Defense-in-Depth provides a risk-informed framework to delineate the scenarios that the plant design features could be exposed to, as well as a framework for defining processes that contribute to defense-in-depth. The scenario framework defines the challenges to the plant safety features that are to be included in the plant design basis and the scope of all deterministic and probabilistic safety evaluations that will be needed to support a plant life cycle risk management program. This framework is useful for the incorporation of information and insights from the PRA and to the formulation of strategies that can be implemented in both the ***Design*** and ***Process Defense-in-Depth*** elements. The elements of ***Scenario Defense-in-Depth*** are listed in Table 4.

Table 4 Elements of *Scenario Defense-in-Depth*

- Comprehensive set of challenges to Barrier Integrity (from a PRA)
  - Internal event scenarios
  - Internal plant hazard scenarios
  - External events scenarios
- Evaluation of Accident prevention strategies
  - Strategies to prevent initiating events
  - Strategies to prevent initiating events from progressing to accidents
  - Strategies to prevent accidents from exceeding the design basis
- Evaluation of Accident mitigation strategies
  - Strategies to reduce frequency of challenges to safety systems
  - Strategies to limit impact of challenges to barriers
  - Strategies to retain and delay transport of radionuclides from barriers during accidents
    - Retention and delay within fuel elements
    - Retention and delay within coolant pressure boundary
    - Retention and delay within containment
    - Strategies to provide offsite protective actions
- Risk management strategies
  - Configuration risk management strategies
  - Change risk management strategies
  - Optimization of safety resources with respect to risk and cost

The overall strategy of the use of scenarios to develop specific strategies to prevent and mitigate accidents is based on the definition of defense-in-depth developed by the IAEA [7,8,9] and is illustrated in Figure 3. This figure if taken too literally may imply a level of defense-in-depth that is more extensive than has actually been implemented in the current generation LWR plants. That is to say each box in the figure does not imply that a separate and independent level of defense-in-depth is applied for each successive failure of in the previous steps. The application of defense-in-depth in current generation plants in the context of independent layers of these lines of defense has been largely constrained to the design basis accidents. An understanding of how defense-in-depth is applied in severe accidents beyond the design basis requires the examination of a suitable spectrum of scenarios from a PRA. Despite these clarifications, the Scenario Defense-in-Depth framework advanced by the IAEA [9] provides a useful model to examine how specific design features contribute to the prevention and mitigation of accidents as will be demonstrated in the next section. Whereas design and process defense in depth are primarily responsible for implementing strategies for managing risks, scenario defense-in-depth provides the means of identifying strategies and for evaluating their effectiveness in both deterministic and probabilistic safety evaluations.

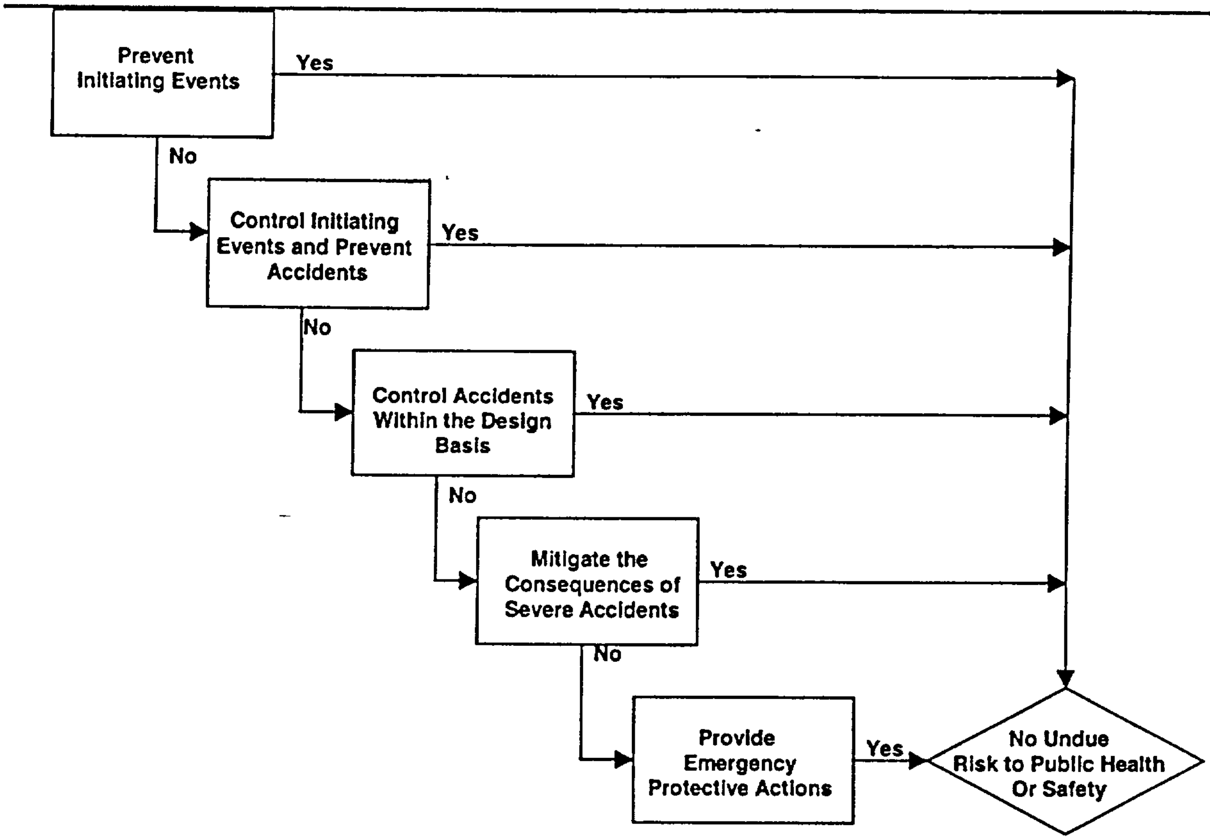

Prevent Initiating Events
Yes
No
Control Initiating Events and Prevent Accidents
Yes
No
Control Accidents Within the Design Basis
Yes
No
Mitigate the Consequences of Severe Accidents
Yes
No
Provide Emergency Protective Actions
Yes
No Undue Risk to Public Health Or Safety

Figure 3 Scenario Defense-in-Depth Framework of IAEA [7,8,9]

Use of PRA to Support *Scenario Defense-in-Depth*

The concepts embodied in ***Scenario Defense-in-Depth*** contribute to defense-in-depth by implementing a comprehensive risk management program that in itself does not provide safety but is needed to measure how well safety requirements are met. Such a program is also needed to "risk inform" the decisions made in ***Design*** and ***Process Defense-in-Depth***. The foundation of the risk management program is a living Probabilistic Risk Assessment that identifies a reasonably complete set of accident sequences for the plant, estimates the frequencies and radiological consequences of these sequences, with a quantification and characterization of the uncertainty in these frequency and consequence estimates. The PRA provides important inputs to the designers and the regulators to specify the licensing basis events that lay the foundation for the safety case and establish that top level regulatory criteria are met. When taken to its fullest capability, the PRA can be used to establish system reliability targets and to evaluate changes to the plant design and operation throughout the plant life cycle. PRA has also been demonstrated its usefulness in interpreting the safety significance of reactor incidents and accidents and the results of regulatory inspections as part of the NRC accident precursor and risk-informed oversight programs.

PRA Framework for Defining Prevention and Mitigation Strategies

The PRA has an important role to play in the defense-in-depth framework as it provides an objective way to identify the roles that each plant safety feature plays in the prevention and mitigation of accidents and to examine how these risk management strategies are balanced. As will be demonstrated in the following, the PRA can be used to provide some clarity of the meaning of prevention and mitigation, in contrast with the current definitions of defense-in-depth.

An accident sequence can be described in terms of the following elements for any reactor concept:

1. An initiating event that constitutes a challenge to the plant systems and structures responsible for control of transients and protection of the plant SSCs including the radionuclide transport barriers.
2. The response (successes and failures) of plant active systems that support key safety functions responsible for protection of barriers, retention of radioactive material, and protection of the public health and safety, as defined by the accident sequence.
3. The response of passive design features responsible for supporting key safety functions, including the structures that form the radionuclide transport barriers themselves and the passive systems that support them.
4. The response of each barrier to radionuclide transport from the radioactivity sources to the environment to the initiating events and safety system responses. This response is expressed as the degree of retention of radioactive material for each barrier expected for the sequence; these barriers include the fuel elements, the primary coolant pressure boundary, and the containment or confinement structure.
5. The implementation of emergency plan protective actions to mitigate the radiological consequences of a given release from the plant.

In the NRC definition of prevention and mitigation presented in SECY 00-198, the above generalized framework is simplified by restricting the safety functions covered in items 2 and 3 to those that prevent core damage, which has a specific meaning to the case of LWRs. However, the point along an accident sequence that one chooses to talk about prevention vs. mitigation is arbitrary. For example, if the point of accident initiation is chosen, then actions to reduce the frequency of an initiating event may be regarded as prevention, while any feature that reduces the probability of failure of systems and structures or magnitude of release at steps 2 through 5 would constitute mitigation of the consequences of the initiating event. Moreover, the use of passive design features that limit the release from the fuel when active systems are postulated to fail could be equally regarded as preventing large releases as mitigating the consequences of active system failures. Hence, while there is a precedent for using core damage as a natural pinch-point for discussing prevention and mitigation for LWRs, the more generalized accident sequence framework leads to the definition of a more general set of damage states for any reactor concept.

The development of a generic reactor framework for discussing accident prevention and mitigation makes use of the following key PRA insights:

1) Absolute prevention of accident would imply that the frequency of the accident is zero, i.e. impossible. However, the PRA approach is not to prove impossibility but to assume possibility and to estimate the frequency. Hence, design features and characteristics that reduce the frequency of a given accident are viewed from the PRA perspective as contributing to prevention. Those that prevent or reduce the level of consequences as viewed from a particular point along an accident sequence are viewed as contributing to mitigation.
2) A given design feature that contributes to prevention, mitigation, or both exhibits varying degrees of importance on different accident sequences. Hence it is necessary to examine a spectrum of sequences some of which may include successful operation of the feature and others that postulate its failure to understand the safety significance of the design feature.
3) A design feature may be postulated to fail along one sequence, but operate successfully on another so it may prevent an accident in some cases and mitigate an accident in others. Hence the extent to which risk is managed by prevention or mitigation by a given design feature varies across the accident sequence spectrum.

A generalized model for describing an accident sequence in terms of the design features that support prevention and mitigation reflecting the above insights is provided in Table 5. This table provides an important feedback mechanism between Scenario and Design Defense-in-Depth. Another important aspect of this model is the separation of plant responses to distinguish between active and passive design features that are used to support safety functions and to implement both prevention and mitigation aspects of the defense-in-depth concept. This sequence model is organized to first identify the response of each active and passive feature by noting which systems and structures are successful and which are postulated to fail along a given accident sequence. For those features that are postulated to fail along the sequence, the design features that contribute to their reliability and thereby reduce the frequency of the sequence are viewed as contributing to accident prevention. Those design features and characteristics of systems and structures that are postulated to function successfully or at least partially successful along the accident sequence, including the response of each of the barriers in limiting the magnitude of the release and the capability of implementing emergency planning measures, are regarded as contributing to accident mitigation. This is true since the operability of the successful systems and structures and the passive features of the barriers do not reduce the accident frequency, but rather help determine the magnitude of the consequences of the accident.

Table 5 Event Sequence Model of Prevention and Mitigation

Standard Elements of Accident Sequence	Design Features Contributing to Prevention	Design Features Contributing to Mitigation
Initiating event	High reliability of SSCs supporting power generation reduce initiating event frequencies; successful operation of the SSCs prevents the sequence	None
Response of active SSCs supporting safety functions: successful and failed SSCs	High reliability and availability of active failed SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence	Capabilities of active successful SSCs reduce the impacts of the initiating events and reduces the challenges to barrier integrity.
Response of passive features supporting safety functions: successful and failed SSCs.	High reliability and availability of passive failed SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence	Capabilities of passive successful SSCs reduce the impacts of the initiating events and reduces the challenges to barrier integrity.
Fraction of source term released from fuel, if any	None	Inherent capabilities of the fuel given successful active or passive SSCs limit the release from the fuel.
Fraction of source term released from the coolant pressure boundary, if any	None	Inherent capabilities of the pressure boundary given successful active or passive SSCs and the capabilities of the fuel limit the release from the pressure boundary.
Fraction of source term released from containment or confinement, if any	None	Inherent capabilities of the containment conditioned on the successful response of any active or passive SSCs along the sequence and the capabilities of the fuel and pressure boundary limit the release from the containment.
Time to implement emergency plan protective actions.	None	Inherent features and capabilities of the fuel, core, pressure, and confinement conditioned on the successful response of any active or passive SSC along the sequence dictate the time available for emergency response.

The accident sequence framework for evaluating accident prevention and mitigation in Table 5 can be used to define a simple model for estimating the risk of a release of radionuclides associated with a specific accident sequence:

$$R_j = Q * F_{IE} * P_{ActiveSSC,j} * P_{PassiveSSC,j} * r_{fuel,j} * r_{PB,j} * r_{cont,j} \tag{1}$$

where:

R_j= *Expected quantity of radioactive material released per year from sequence j*

Q= *Quantity of radionuclides (for a given isotope) in the reactor core inventory*

F_{IE}= *Frequency of the initiating event associated with sequence j*

$P_{ActiveSSCJ}$= *Probability of the successful and failed active SSCs along sequence j*

$P_{PassiveSSCJ}$= *Probability of the passive structure successes and failures along sequence j*

$r_{fuel,j}$= *Release fraction from the fuel, given system and structure response for sequence j*

r_{PB_J}= *Release fraction from the PPB, given system and structure response for sequence j*

r_{cont_J}= *Release fraction from the confinement, given system and structure response for sequence j*

Each probability term in the right-hand side of this equation depends on the events that precede it along the sequence as would be included in a competent PRA model. The partitioning of the risk into these specific terms is designed to support an evaluation of specific strategies for preventing and mitigating the risks of accidents. In view of the large uncertainties inherent in attempts to quantify the risk of low frequency accidents, the quantification of Equation (1) cannot be done with high precision. However the application of the equation to explore defense-in-depth only requires rough order of magnitude estimates. Such rough estimates are all that is needed because the accident spectrum encountered in a PRA spans many orders of magnitude of accident frequency and release fractions. The equation is only used to develop insights regarding how design features and barriers are expected to perform along specific sequences. Any deterministic or risk informed decision that is made to license or regulate a new reactor concept must at least make some assumptions regarding the magnitude of these quantities if even a qualitative conclusion about the risk to public health and safety is to be made.

Note that each term on the right hand side of Equation (1) whose value is less than unity can be regarded as a "risk reduction factor". If we start with the inventory Q and consider that the upper bound frequency of releases from this inventory is once per year[6], then each factor contributes to reducing the risk of a release. By noting the SSCs that correspond to each factor, this equation can be used to quantify the importance of each design feature in managing the risk for the associated sequence.

In the above formulation, highly reliable SSCs responsible for producing electric power and keeping the plant in stable conditions reduce the frequency of initiating events and thereby prevent accidents from initiating. Highly reliable and available SSCs that are postulated to fail along the accident sequence manage the risk by reducing the values of $P_{systems,j}$ and $P_{structures,j}$. Hence the reliability characteristics of these systems prevent accidents. SSCs that are postulated to be successful along the sequence in the PRA model help reduce the loads on the barriers and together with the inherent features of the barriers help to reduce the release fractions. The capabilities of these systems and structures when successful help to mitigate the consequences of the accidents. When a necessary and sufficient combination of successful SSCs meets the success criteria for the protection of each barrier, releases from that barrier are prevented. By examining the values of the response probabilities and the release fractions along each accident sequence that determines the risk profile, the role of design features in contributing to prevention and mitigation of accidents can be objectively quantified. When this process is applied to a representative set of accident sequence families that characterize the overall risk profile, a comprehensive assessment of the importance of each design feature in preventing and mitigating accidents is achieved. While the uncertainties that are inherent in estimating each of the factors in the equation are large, the objective is not an accurate allocation, but rather a rough order of magnitude feel for the relative importance of each design feature in contributing the prevention and mitigation of accidents.

In the following sections this approach of defining and evaluating design features that support prevention and mitigation strategies is applied to sets of sequences for two different reactor types, the PWR and the MHTGR. These examples were selected for several reasons: 1) they cover one of the existing LWR concepts with which we have the most experience in applying the definitions of defense-in-depth and one advanced reactor concept that has inherent characteristics fundamentally different than the existing LWRs; 2) The former example uses a conventional leak tight containment concept whereas the latter uses a non-leak tight confinement; 3) the current PWR design uses conventional active safety systems to perform critical safety functions such as decay heat removal, whereas the MHTGR uses a combination of active and passive safety systems including a decay heat removal capability that is independent of any active components; and 4) each has available a peer reviewed PRA to support the application that includes a full quantification of uncertainties, to the extent that such uncertainties are treatable within the scope of a competent PRA. These examples are not used to develop any definitive conclusions about the adequacy of any particular design or reactor concept but to demonstrate the concepts of defense-in-depth and prevention and mitigation evaluation advanced by this paper. The ultimate goal is to

[6] While there is no theoretical upper bound for an event frequency, this is a practical upper bound for a severe accident because the first such accident in any year will certainly be the last for that year and for the plant lifetime if any appreciable fraction of the core inventory is released.

develop a better understanding of the ways in which each reactor has implemented defense-in-depth concepts to prevent and mitigate selected accident sequences that are representative of the respective PRA results. Although this approach puts the definition of prevention and mitigation in the framework of a PRA event sequence model, the authors are not proposing that we abandon the traditional deterministic evaluations of reactor safety. This framework can also be used in the context of design basis accidents that have been established based on engineering judgment. As noted earlier, even if the terms in the above equation are not quantified as one attempts to do in a PRA, some assumptions about the magnitude of each term must be made even within the deterministic framework.

Evaluation of Selected LWR Sequences

To demonstrate this concept of evaluating prevention and mitigation strategies to existing LWRs, three sequences were selected as representative sequences from some of the PWR results in NUREG-1150 [16]. While this sample of sequences analyzed for one isotope does not tell the whole story, these sequences are representative of the results of the supporting PRA and include those that dominate the risk of I-131 releases. These sequences are briefly described as follows:

PWR-1 This is a small LOCA initiated sequence with successful response of the ECCS and hence core damage is assumed to be prevented. As with PWR-2 the containment remains intact during this sequence. The major part of the I-131 inventory remains in the fuel during this sequence as core damage does not occur. The circulating activity in the reactor coolant is released to the containment which retains a large fraction of that in mitigating the releases to environment.

PWR-2 This is a small LOCA initiated sequence with an independent failure of the ECCS in the recirculation mode which requires operator action. The ECCS failure is assumed to result in core damage, but in this sequence the containment remains intact during the sequence retaining a large fraction of the radionuclides that are released from the fuel.

PWR-3 An interfacing systems LOCA sequences caused by failure of two check valves at the interface of the reactor coolant system and the low pressure injection system which results in a loss of coolant outside the containment, and the inability to establish recirculation ECCS functions as the coolant inventory is lost outside the containment. The PRA models this sequence as a core melt with a containment bypass because the release pathway is direct from the coolant pressure boundary to the environment bypassing the containment.

The PRA frequency and release data developed for the evaluation of these sequences was developed from NUREG-1150 for the radionuclide species I-131. A more complete evaluation would need to consider a full set of risk significant sequences and a larger set of radionuclide species, however these three sequences and I-131 provide an adequate example to demonstrate how PRA information can be used to examine design features responsible for prevention and mitigation. A summary of the salient data for these sequences is provided in Table 6. Each of these terms has associated with it an uncertainty distribution, from which the mean values have been selected. These uncertainties can be more than an order of magnitude, especially for the low frequencies and probabilities and the release fractions. In interpreting the results, only the logarithms of these numbers are considered significant in developing insights on the relative importance of plant features in managing risk via prevention and mitigation strategies. Absolute safety margin determinations are outside the scope of this example.

The sequences selected for the PWR examples are representative in that they contain examples of successful and unsuccessful SSC response to protect the fuel barrier and the containment barrier, and all three cases represented examples where the coolant pressure boundary barrier is violated at the initiating event. In PWR-1 the primary role of defense-in-depth is the mitigation effects of retaining the radionuclides in the fuel and in the containment when the fuel barrier and containment barrier are successfully protected. Sequence PWR-2 is a small LOCA with independent failure of the ECCS resulting in core damage and large releases into the containment, but the containment barrier is intact and is not bypassed in this sequence such that containment retention of this fission product is very effective. In PWR-3 the primary role of defense-in-depth is the prevention of the failure of the pressure boundary where an interfacing systems LOCA can take place. This sequence which was originally identified in the Reactor Safety Study results in part from the lack of concentricity of the barriers in the PWR design. As it requires failure of two normally closed check valves in this example, its frequency is very low. However, the resulting core damage and containment bypass

Table 6 Data Assumed for LWR Sequence Evaluation (from Reference [16])

Sequence	PWR-1	PWR-2	PWR-3
Initiating Event	Small LOCA	Small LOCA	Interfacing Systems LOCA
Active SSC Response	Successful ECCS preventing core damage	Failure of ECCS in recirculation mode and core damage	Consequential failure of ECCS and core damage
Passive SSC Response	Containment Intact	Containment Intact	Containment Bypass
Initiating Event Frequency per yr.	~1x10^{-2}	~1x10^{-2}	~1x10^{-6}
Active SSC response probability	~1	8x10^{-4}	~1
Passive SSC response probability	~1	~1	~1
Fractional release of I-131 from Fuel	~2x10^{-6}	~1	~1
Fractional release of I-131 from PB	~1	~1	~1
Fractional release of I-131 from Containment	~2x10^{-4}	~2x10^{-4}	~2x10^{-1}

results in a large fraction of the I-131 inventory in the source term according to the data assumed for this example.

As shown in Figure 4, the frequencies and releases of I-131 for these three selected sequences can be plotted in a frequency consequence plot in a manner that permits the identification of different factors that contribute to accident prevention and mitigation. Also plotted is a point corresponding to the inventory of I-131 for an assumed 300Mwt reactor (coinciding with the size of the modular HTGR example) at a frequency of 1 per year, which is selected to represent the upper bound on the frequency of any accident that involves the release of radioactive material. For each of the three PWR sequences, additional points are defined in which successive mitigation and prevention factors in Equation 1 that participate in the sequence are assumed to be removed in a progressive sequence to permit the characterization of importance of each prevention and mitigation strategy that participates in the sequence.

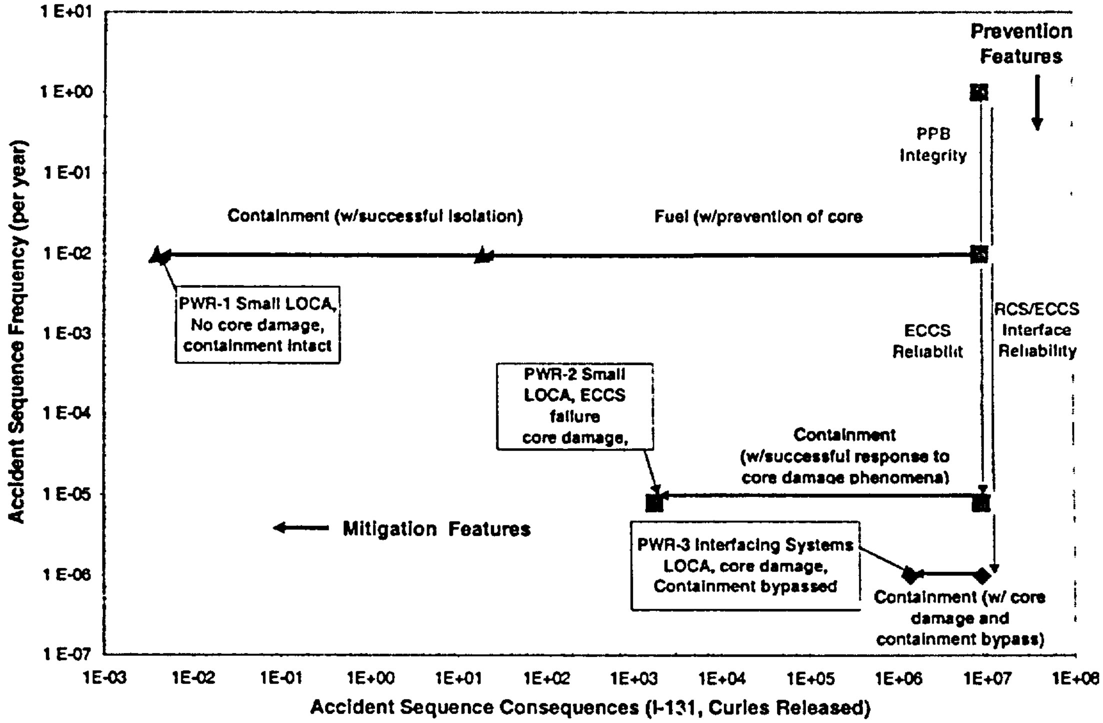


Figure 4 Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected PWR Sequences

This approach is used to estimate the quantitative contribution that each design feature makes to managing the risk of associated with an annual release of the I-131 inventory in relation to the risk of an annual release of the inventory. Information presented in this plot is used to develop the bar chart in Figure 5 which identifies the role of design features in determining the risk of an I-131 release for each sequence. The risk reduction factor quantified in Figure 5 corresponds to the order of magnitude (i.e. logarithim of the) reduction in risk computed by the risk reduction factors of Equation (1) associated with each design feature. The design features associated with prevention are those that contribute to lowering the frequency in relation to 1 occurrence per year. Those that contribute to mitigation are those that contribute to reducing the fraction of I-131 that is released in relation to the core inventory of I-131.

As seen in Figure 5, for Sequence PWR-1 the reliability of the coolant pressure boundary as a prevention feature is responsible for a 2 order of magnitude effect in managing the risk, whereas there is a 9 order of magnitude impact of mitigation features that help limit the magnitude of the source term for this sequence. This reduction is provided by the fuel barrier (>5 orders of magnitude) and the containment barrier (>3). For Sequence PWR-3, the interfacing pressure boundary contributes 6 orders of magnitude of prevention from the design features that reduce the likelihood of such a sequence, but there is only about 1 order of mitigation as there is core damage and a containment bypass condition. Only in Sequence PWR-2 is there a relative balance in the strategies of prevention and mitigation when viewed from this perspective, with 2 orders of magnitude prevention by the pressure boundary reliability, 3 orders of prevention by the ECCS reliability, and almost 4 orders of mitigation by the containment. A characteristic of these results that is typical for LWRs is that there is significant retention of radionuclides within the fuel barrier only when core damage is prevented. Another is, as discussed previously, that when the fuel barrier is postulated to fail as occurs in the core damage sequences, the coolant pressure boundary plays an insignificant role in risk mitigation. These LWR examples as well as the MHTGR examples presented in the next section clearly show that the extent of balance is highly sequence dependent.

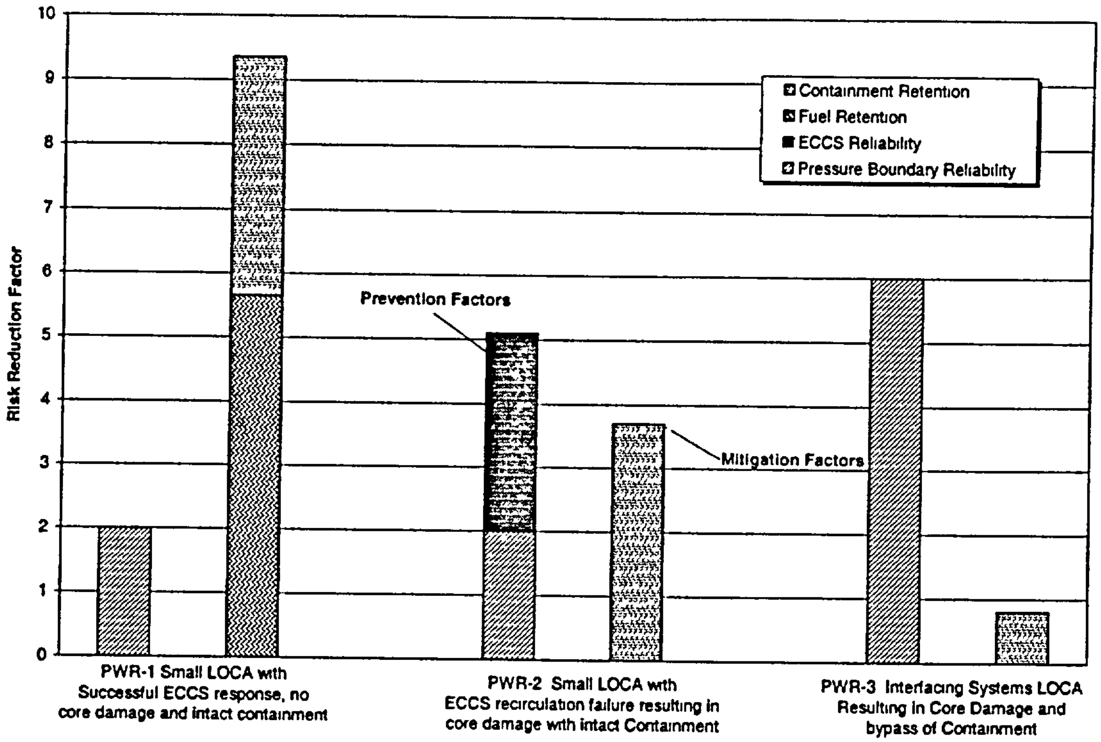


Figure 5 Risk Reduction Factors Associated with PWR Design Features Responsible for Prevention and Mitigation of I-131 Releases

Evaluation of Selected MHTGR Sequences

To demonstrate the application of these concepts to advanced reactors with fundamentally different characteristics than LWRs examples from the MHTGR PRA [17] are used. This MHTGR design has a package of inherent and engineered safety features that are representative of various modular gas cooled reactor designs using particle fuel, graphite moderator, helium working fluid, and passive decay heat removal capabilities that includes the PBMR [15]. A more complete description of the inherent and engineered safety features in these gas cooled reactors is presented in Reference [15]. The numerical data used for these examples is taken from Reference [17] and is summarized in Table 7. As with the PWR sequences, this sample of MHTGR sequences analyzed for one isotope does not tell the whole story. However these sequences are representative of the results of the supporting PRA and include those that dominate the risk of I-131 releases.

Table 7 Data Assumed for MHTGR Sequence Evaluation (from Reference [17])

Sequence	MHTGR-1	MHTGR-2	MHTGR-3
Initiating Event	Moderate Helium Pressure Boundary Failure	Small Helium Pressure Boundary Failure	Small Helium Pressure Boundary Failure
Active SSC Response	Successful Helium pump-down and forced circulation cooling	Successful Helium pump-down, Failure of forced circulation cooling systems	Failure of forced circulation cooling systems
Passive SSC Response	Successful confinement response	Success of passive core cooling system and confinement	Failure of passive core cooling system
Initiating Event Frequency per yr.	$8x10^{-3}$	$\sim3x10^{-2}$	$\sim3x10^{-2}$
Active SSC response probability	.8	$\sim5x10^{-3}$	$\sim5x10^{-3}$
Passive SSC response probability	~1	~1	$\sim3x10^{-6}$
Fractional release of I-131 from Fuel	$\sim2x10^{-6}$	$\sim2x10^{-5}$	$\sim6x10^{-5}$
Fractional release of I-131 from PB	$\sim1x10^{-3}$	$\sim4x10^{-1}$	$\sim5x10^{-1}$
Fractional release of I-131 from Containment	$\sim3x10^{-1}$	$\sim4x10^{-2}$	$\sim4x10^{-2}$

MHTGR-1 Moderate size leak in the Helium Pressure Boundary (HPB) of less than 13 in^2 ; successful reactor trip and continued operation of one of the forced convection cooling systems; releases limited to circulating activity and some lift off of plated out radionuclides.

MHTGR-2 Small leak in the HPB of less than 1 in^2; successful reactor trip, failure of the active forced convection cooling systems; conduction cool down of the core using the active Reactor Cavity Cooling System (RCCS); releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles that is minimized due to the successful HPB pump down along this sequence

MHTGR-3 Small leak in the HPB of less than 1 in^2; successful reactor trip; failure of the active forced convection cooling systems; failure of the active RCCS; conduction cool-down to the passive reactor cavity heat sinks; releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles (somewhat larger fraction than in Sequence [2])

The risk plots and bar charts for these MHTGR sequences that parallel the development for the PWR sequences are shown in Figures 6 and 7.

As seen in these figures the roles of prevention and mitigation for MHTGR-1 are similar to PWR-1 with 2 orders of magnitude of prevention by the reliability of the coolant pressure boundary, and 9 orders of magnitude of mitigation by the barriers, although in this sequence there is less of importance of the containment, as the MHTGR design employs a non-leak tight confinement concept. However the pressure boundary retention in the form of plateout for this sequence compensates for any lack of retention from use of a non-leak tight confinement.

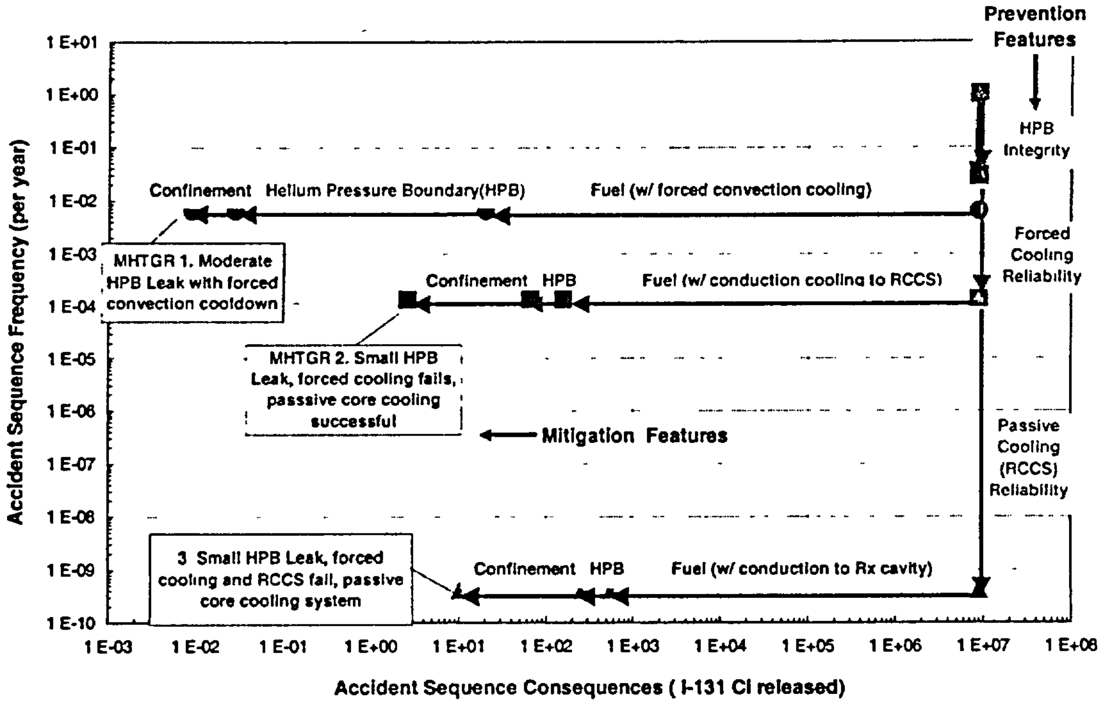


Figure 6 Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected MHTGR Sequences

MHTGR-2 has some functional similarities with PWR-2 in that both involve a small breach in the pressure boundary followed by failure of the active SSCs supporting core cooling functions. However the mitigation level for this sequence is aided by a passive core cooling capability that prevents significant releases from the fuel, although the releases are somewhat higher than in Sequence MHTGR-1. In MHTGR-3 there is failure of both active and passive core cooling systems following the pressure boundary breach, but the passive capability of the reactor to retain its fuel inventory is still significant as the core is still cooled by conduction and radiation to the reactor building heat sinks. What is striking about the prevention and mitigation analysis for these MTHGR sequences is that the mitigation importance of the fuel retention never drops below 4 orders of magnitude and the total mitigation significantly below 6 orders of risk reduction despite the use of a non-leak tight confinement.

While one can use this process to attribute and quantify the importance of specific design features in preventing and mitigating accidents, it is important to note that the assessment of risk for any sequence for any reactor type is a function of how the inherent features and engineered features respond to the initiating event and interact with each other to produce the definition, frequency, accident progression and consequence of the scenario. In particular the role and importance of leak tight containments in implementing the defense-in-depth concept cannot be determined outside of the context of the inherent features, particularly those that determine the fuel performance under accident conditions. This integrated perspective of risk factors is an important principle of ***Scenario Defense-In-Depth*** that is essential to defining and evaluating prevention and mitigation stragies.

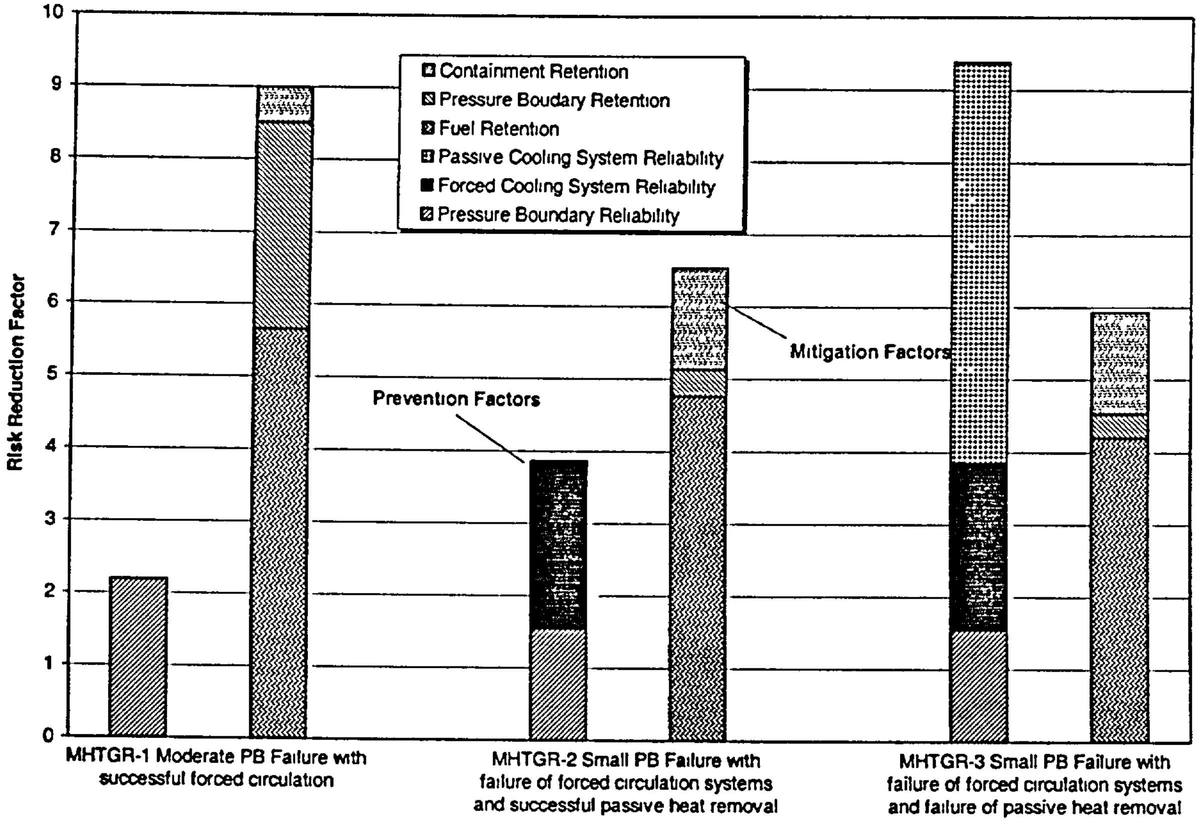


Figure 7 Risk Reduction Factors Associated with PWR Design Features Responsible for Prevention and Mitigation of I-131 Releases

Upon review of two sets of sequences for two fundamentally different reactor concepts, it is instructive to review some of the elements of the earlier definitions of defense-in-depth. Several conclusions can be reached for these examples:

- There exists no single "balance" between prevention and mitigation as the roles of these strategies are inherently different for different sequences. High frequency/low consequence accidents exhibit less prevention and more mitigation, and vice versa for lower frequency, higher consequence accidents.
- There is no such thing as independent barriers to radioactivity release, as all the barriers are mutually dependent on the inherent features of the reactor and how these features interact with the respective barriers, which is different on different sequences.

- By design the fuel barrier provides an important contribution to accident mitigation on all analyzed MHTGR sequences, whereas this barrier is only significant on the PWR sequences in which no core damage occurs. This affirms the logic of focusing on core damage prevention and mitigation in application of defense-in-depth strategies for LWRs. In addition the capabilities of the fuel barrier as reflected in the PRA results for these MHTGR are seen to compensate for the lack of leak tight containment in terms of supporting the strategy to mitigate accident consequences.

As a final comment on this section the authors acknowledge that there are large uncertainties inherent in the PRA results that were used to support these examples. Hence, if one varies the PRA inputs selected for these examples, listed in Tables 6 and 7, different results and conclusions would be obtained. The only purpose of presenting these examples is to demonstrate how PRA results can be used to examine and quantify the importance of specific design features in preventing and mitigating severe accidents. These order of magnitude estimates of risk reduction factors using PRA techniques are only intended to provide rough order of magnitude estimates of importance. Nonetheless, such estimates are believed to incorporate risk insights not present in the currently available definitions of defense-in-depth.

Having said that, the authors do not propose that defense-in-depth philosophy be revised to a fully risk based approach, only that the definitions be revised to incorporate risk insights more fully into the original deterministic framework.

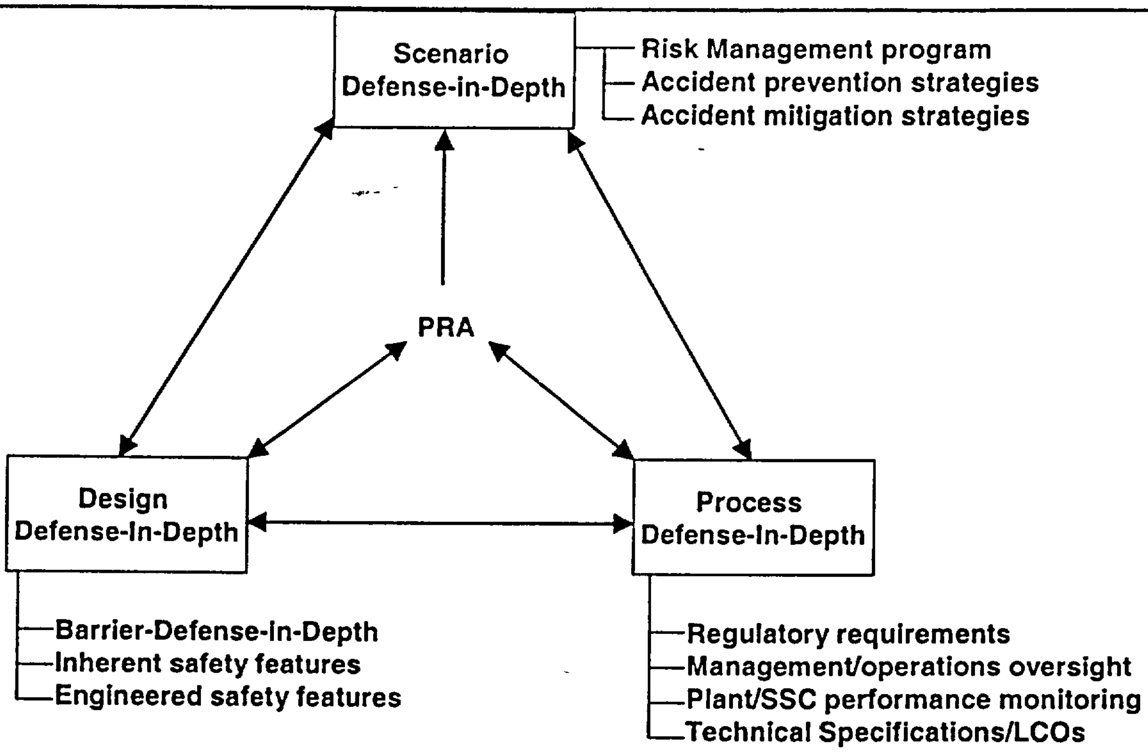
SUMMARY AND CONCLUSIONS

In summary, a review of the published definitions of defense-in-depth was performed to support the design and licensing of advanced reactor concepts such as the MHTGR and PBMR. The existing defense-in-depth definitions have been consistent in calling for multiple lines of defense in protecting the health and safety of the public. Our review of these definitions has identified a number of issues including a lack of consistency and the total lack of visibility of role the inherent reactor features in supporting the defense-in-depth concept. A number of risk insights were identified that challenge some of the precepts of the existing risk informed definitions of defense-in-depth. These insights include the fact that barrier independence is beyond the capabilities of current reactor designs and that prevention and mitigation strategies are not balanced but rather are applied to different extents along different accident sequences. These issues were used to support a proposal for a revised definition of defense-in-depth that can be used for all reactor concepts including those with fundamentally different characteristics than the current generation LWRs.

The proposal for a revised definition suggests the need for three distinct types of defense-in-depth including ***Design, Process***, and ***Scenario Defense-in-Depth.*** Design Defense-in-Depth focuses on strategies implemented during the design phase including the selection of inherent features, definition of reactor specific safety functions, and passive and active engineered safety features that together with the inherent features support the maintenance of radionuclide barriers. ***Process Defense-in-Depth*** sets requirements and criteria for decisions that are made in the life cycle of the plant that contribute to plant safety and is the focus of many regulatory decisions to support licensing and regulation of nuclear power. ***Scenario Defense-in-Depth*** provides a framework for the evaluation of safety using appropriate combinations of deterministic and probabilistic approaches and serves as the "referee" in determining how well the ***Design*** and ***Process Defense-in-Depth*** decisions are implemented. These elements are supported by a comprehensive ***PRA*** and mutually support each other in this risk informed framework that is illustrated in Figure 8.

In proposing this new definition of defense-in-depth, the authors attempt to address several issues with the existing definitions that are discussed at the beginning of this paper and to provide a more general framework that can be applied to advanced reactors as well as current generation LWRs. This definition incorporates the main features of the existing definitions, proposes some new elements, and attempts to rearrange them to provide a more complete explanation of the role of defense-in-depth in providing the overall safety of a particular reactor concept.

Design Defense-in-Depth includes the inherent features of the reactor, independent and concentric radionuclide barriers, and engineered safety features to support the integrity of these barriers. Engineered safety features include operator actions and the use of both active and passive systems and perform reactor specific safety functions to protect barrier integrity. ***Process Defense-in-Depth*** captures the development of requirements governing all decisions made in the design, licensing, operation, maintenance, testing, inspection, management and oversight.


Scenario Defense-in-Depth
Risk Management program
Accident prevention strategies
Accident mitigation strategies
PRA
Design Defense-In-Depth
Process Defense-In-Depth
Barrier-Defense-In-Depth
Inherent safety features
Engineered safety features
Regulatory requirements
Management/operations oversight
Plant/SSC performance monitoring
Technical Specifications/LCOs

PRA – Probabilistic Risk Assessment
RM – Risk Management

LCO – Limited Condition for Operation
SSC – Structure, System, Component

Figure 8 Comprehensive Defense-In-Depth Framework

Scenario Defense-in-Depth includes the development and evaluation of strategies to prevent and mitigate the consequences of accidents. It is supported by a comprehensive living PRA and risk management program that can be used to quantify the importance of each element of the design in preventing and mitigating accidents. This evaluation feeds back important risk insights to ***Design and Process Defense-in-Depth*** completing a mutually supporting cycle of defense-in-depth activities.

All the decisions that are made to implement defense-in-depth are supported by a comprehensive and living PRA that is used to identify the design basis challenges to the radionuclide barriers and to evaluate these decisions against quantitative decision criteria. As with the current definitions, defense-in-depth strategies such as safety margins are applied to address uncertainties and limitations in our state of knowledge including that which is reflected in the PRA results.

The authors have also proposed a risk-informed framework to define and evaluate the role of plant design features in preventing and mitigating accidents. This framework was demonstrated on selected representative LWR and MHTGR sequences. The ultimate goal of these proposals is to add clarity to the application of defense-in-depth concepts to the design, licensing, and life cycle management of advanced reactor concepts.

REFERENCES

[1] S. Glasstone and A. Sesonske, *Nuclear Reactor Engineering,* C1967 Van NOstrand., pp. 25-27

[2] D. Okrent, *Nuclear Reactor Safety – On the History of the Regulatory Process,* C1981 University of Wisconsin Press

[3] J.N. Sorensen, G.E. Apostolakis, T.S. Kress, and D.A. Powers, " On the Role of Defense-in-Depth in Risk Informed Regulation", presented at PSA '99, Washington DC, August 22-25, 1999, American Nuclear Society, La Grange Park, Illinois, USA.

[4] C. Beck, "Basic Goals of Regulatory Review: Major Considerations Affecting Reactor Licensing," Statement submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on Licensing and Regulation of Nuclear Reactors, April 4,5,6,20, and May 3, 1967.

[5] Internal Study Group, "Report to the Atomic Energy Commission on the Reactor Licensing Program," submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on AEC Licensing Procedure and Related Legislation, June 1969.

[6] F. E. Haskin, and A. L. Camp,, "Perspectives on Reactor Safety," NUREG/CR-6042, Nuclear Regulatory Commission, Washington, DC, March 1994.

[7] International Nuclear Safety Advisory Group, "Basic Safety Principles for Nuclear Power Plants," Safety Series No. 75-INSAG-3," International Atomic Energy Agency, Vienna, Austria, 1988

[8] International Nuclear Safety Advisory Group, "Defense in Depth in Nuclear Safety," INSAG- 10, International Atomic Energy Agency, Vienna, Austria, 1996

[9] A. Carnino and M. Gaparini, " Defence in Depth and Develoment of Safety Requirements for Advanced Reactors", Workshop on Advanced Nuclear Reactor Safety Issues and Research Needs, Paris, February 18-20, 2002

[10] Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Current Licensing Basis", January 1988.

[11] SECY 00-198, Attachment 1, "Framework for Risk Informed Changes to the Technical Requirements of 10 CFR 50", Draft Revision 2, August 2000.

[12] D. E. Akers, et al, "Three Mile Island Unit 2 Fission Product Inventory Estimates", Nuclear Technology, Vol. 87,, August 1989.pp. 205-213

[13] A.M. Weinberg, et al, *The Second Nuclear Era – A New Start for Nuclear Power*, C1985 Praeger Publishers.

[14] "Policy for the Regulation of Advanced Nuclear Power Plants," USNRC, 51FR24643, July 1986.

[15] Exelon Power Corporation, "Proposed Licensing Approach for the Pebble Bed Modular Reactor in the United States.", March 2002

[16] "Reactor Risk Reference Document," USNRC, NUREG-1150, Volume 1, February 1987.

[17] "Probabilistic Risk Assessment for the Standard High Temperature Gas-Cooled Reactor," Department of Energy, DOE-HTGR-86011, Revision 5, April 1988.