Enhancement of the Use of Defense-in-Depth and Safety Margin for Decision-Making Purposes

Fernando Ferrante[a], Karl Fleming[b], Ed Parsley[c], Charlie Young[c], and Leo Shanley[c]
[a] Electric Power Research Institute, Charlotte, North Carolina, United States, fferrante@epri.com
[b] KNF Consulting Services LLC, Spokane, United States, karlfleming@comcast.net
[c] Jensen Hughes, West Chester, United States, eparsley@jensenhughes.com, cyoung@jensenhughes.com, lshanley@jensenhughes.com

Abstract: Both Defense-In-Depth (DID) and Safety Margin (SM) have been longstanding key concepts in nuclear applications, well before Probabilistic Risk Assessment (PRA) became a staple of risk applications in this field. A detailed review of key references about DID/SM in RIDM indicates that these topics are overdue for a more efficient, integrated approach, as RIDM applications continue to gain acceptance and implementation experience worldwide. As the use of PRA and RIDM continues to expand, different perspectives on DID/SM can challenge the incorporation of additional risk modeling and wider, more comprehensive application of PRA in nuclear power plants (NPPs). Challenges from a deterministic-oriented perspective against more risk-informed applications, as well as their expansion in areas where PRA is not used as heavily, can lead to misperceptions that DID/SM principles are not aligned with respect to risk insights obtained via risk assessment inputs. A careful investigation and discussion of DID/SM as overarching principles of nuclear safety was performed to highlight that they are not intended to be substituted by PRA methods, tools, and results. Rather, the approach is to derive key elements of DID (i.e., design, programmatic, and scenario-based) that also accounted for SM inputs in a more logical, structured manner. Several key conclusions were derived from this investigation, including the need for an enhanced, more efficient approach. Using key characteristics on how to treat DID/SM in RIDM, a recommended framework for an improvement implementation of DID/SM in RIDM is proposed, recognizing that DID/SM aspects are essential nuclear safety principles. As a different perspective than typically applied in current RIDM guidance, SM is identified as a fundamental input into the DID principle that can be better contextualized in RIDM as a supporting element (rather than a distinct and separate element). A significant discussion of how design, programmatic, and scenario-based DID aspects can be used in areas where PRA insights are already heavily used as well as in other areas not traditionally reliant on such inputs is discussed (including qualitative as well as quantitative risk inputs). A modern PRA model from an existing NPP site is used to showcase how risk insights on the achievement and preservation of DID/SM apply in the context of RIDM. The overall approach was based on leveraging existing guidance worldwide, considering approaches that appropriately bring the information together in a practical manner, as well as an investigation with actual implementable examples

1. INTRODUCTION

Defense-in-Depth (DID) and Safety Margins (SM) are key principles associated with nuclear safety, in general, as well as in risk-informed decision making (RIDM). Recently, EPRI produced a report (EPRI 3002014783 [1]) which discusses the roles of DID and SM within an Integrated RIDM framework (IRIDM). This was followed by an in-depth report on DID/SM in RIDM that is the basis for the work presented here (EPRI 3002020763 [2]).

Initially, for many reactor applications, the level of DID/SM tended to be assumed as being significantly robust (and, therefore, not impacted) or the risk results were sufficiently below thresholds such that satisfying these principles was not considered an issue. As the use of PRA and RIDM continued to expand, the incorporation of additional risk modeling and the use of PRA for a wider, more

comprehensive use in nuclear power plant (NPP) operations has led to additional scrutiny and level of effort on justifying the adequacy of risk results (especially when the calculated changes in risk are close to regulatory thresholds for risk criteria). In addition, increasing questions on DID/SM with respect to individual applications (often without clear guidance on how to address such questions) have come up. Finally, challenges from a deterministic-oriented perspective against traditional risk-informed applications still occur, where the concepts of DID/SM can often be interpreted as being out of alignment with respect to risk assessment results.

While significant guidance in RIDM exists, the impact of DID/SM is not always as clear as principles such as comparison of quantitative risk results against criteria. For example, in the U.S., additional guidance on DID and SM evaluation has been integrated into key regulatory documents 2018 [3]. This revised guidance also has raised expectations that future RIDM applications will provide a more systematic demonstration that the principles of DID and SM have been preserved.

2. LITERATURE OVERVIEW OF DID/SM IN RIDM

A significant range of literature on the topic of DID/SM has been published by safety authorities, research groups, and other organizations. The available references cover different perspectives on the definitions of DID/SM, how they are taken into account in RIDM, and how the adequacy of DID/SM can be evaluated. It should be noted that the references discussed in subsections 3.1 and 3.2 are a subset of the references and topics discussed under a much more expansive literature review in EPRI 3002020763 [2], so they have been significantly summarized here.

3.1. Regulatory References

A comprehensive review of the U.S. and international literature on DID was performed by the NRC staff and published in 2016 as NUREG/KM-0009 [4]. One of the goals of NUREG/KM-0009 was to capture a historical review and perspectives of DID from references dating back to the 1950s. As such, this was a major effort in collecting both key recent documents on the topic, as well as the evolution of the discussions around DID in general. NUREG/KM-0009 clearly states that "over the years, however, DID, … has not been described, discussed or defined consistently" and that this is expected, given that "different authors have invoked the DID concept in ways that best suit the particular purpose of their document." The report identifies that DID has been used in multiple nuclear applications (often with different names) and with various definitions (some of them similar but with the potential for multiple interpretations) around the topics of "layers", "redundancy", "independency", and "multiple barriers" against radiation releases.

A key discussion held through the years on this subject is captured in NUREG/KM-0009, which is essential to the central aspects of the framework proposed in this report. For a significant portion of the initial development of regulatory guidance, the view around DID was dominated by a mostly "structuralist" perspective. Under this perspective, DID tends to be described as meeting the regulatory requirements, which include such DID/SM elements, via protections relying on multiple barriers, the single failure criterion, SMs or other similar concepts.

In contrast, a "rationalist" perspective (and its relation to the "structuralist" perspective) is introduced in discussions after several debates where PRA, DID, and the "structuralist" views are reconsidered (e.g., [5]). The "structuralist" perspective asserts DID is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations, and the "rationalist" perspective asserts DID is the aggregate of provisions made to compensate for uncertainty and incompleteness in the knowledge of accident initiation and progression as reflected in the results of a PRA in relation to the expectations for safety reflected in the safety goals.

These two perspectives are important because they (1) identify different schools of thought (and interpretation – a main challenge with this topic) on the definition and implementation of DID, and (2)

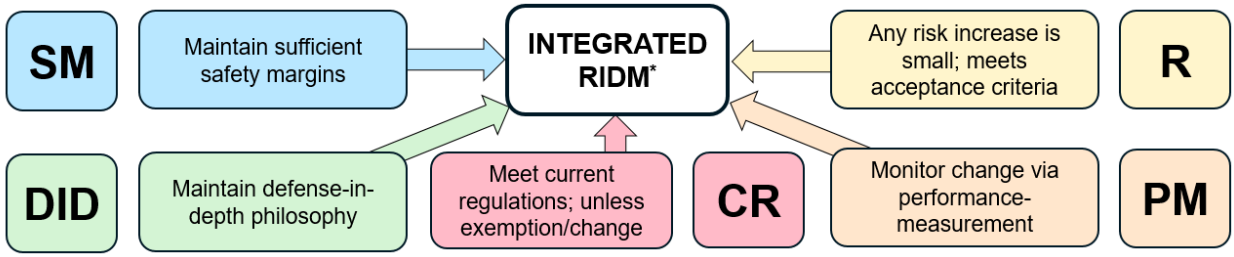
they distinguish potential different approaches to addressing DID. In the "structuralist" perspective, regulations (or any requirement on DID) should be specified explicitly and meeting those requirements, therefore, assures compliance with DID principles. In the "rationalist" perspective, the "aggregate of provisions" is how DID is addressed, with the implicit assumption that uncertainty and incompleteness in the knowledge are accounted for in some manner.

Another fundamental reference in the field of RIDM is the U.S. NRC's Regulatory Guide 1.174 (RG 1.174) Revision 3 [3], titled "An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis". Because of its ground-breaking nature in the use of RIDM in regulatory activities, RG 1.174 is both a key reference in terms of its general discussions as well as an application-specific guidance document with respect to the use of PRA (and RIDM) to allow changes in the licensing basis of the NRC. The discussion in this subsection will limit itself to the former (see Section 2.2.9.1 for details on the latter). The information in RG 1.174 has been discussed in a wide number of references, including EPRI 3002014783 [1] which is a key reference that spurred this work on DID/SM in RIDM.

One of the key bases used in multiple activities beyond the application of RG 1.174 is the description of the Integrated RIDM (or IRIDM [1]) concept as having five key principles as illustrated in Figure 1. The obvious link between RIDM and DID is the fact that it is the subject of one of the five fundamental principles in terms of ensuring any do not challenge the DID philosophy (while SM is another).

While RG 1.174 does not define DID explicitly, it discusses its basic aspects and principles in detail (See Section C2.1.1.1 in [3]). It indicates that DID is not just a principle in terms of licensing changes using RIDM but a general philosophy, in line with prior U.S. NRC references, "that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility".

Figure 1: Illustration of RIDM Principles Presented in U.S. NRC RG 1.174 [3]



More importantly, it also states that NPPs "that leverage the DID philosophy in the design of the plant can gain some flexibility in operations and maintenance" (e.g., testing and maintenance or corrective actions). In other words, DID is not meant to be simply an imposition, but also something that provides flexibility when considered in an integrated fashion with the principles illustrated in Figure 1. It also identifies those temporary changes in the conditions of SSCs are not automatically meant to assume loss of DID (and, therefore, automatically deemed to be not acceptable).

3.2. International References

The International Atomic Energy Agency (IAEA) has multiple references on the topic of DID/SM which are discussed in detail in NUREG/KM-0009. A key document from IAEA guidance is INSAG-10 [6], issued in 1996, which provides the following guidance: (1) DID consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant, and (2) DID is implemented through design and operation to provide a graded protection against a wide

variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant.

An important item to note with respect to some definitions discussed in Section 2.2.1 is that the IAEA definition explicitly calls out "equipment and procedures" as an element of different levels, as well as the various challenges that a plant may experience with respect to DID implementation. Both design and operations are mentioned and the overall approach by IAEA in this document is closer to the "rationalist" perspective than the "structuralist" one. In addition, five specific levels of DID are explicitly defined: (1) prevention of abnormal operation and failures, (2) control of abnormal operation and detection of failures, (3) control of accidents within the design basis, (4) control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents, and (5) mitigation of radiological consequences of significant releases of radioactive materials.

In addition to the DID definition and explicitly defined DID levels (as opposed to focusing on a narrower physical "barriers"-based definition), IAEA INSAG-10 also has important key statements regarding other aspects of DID. It explicitly identifies that DID is not a concept to be applied uniformly, i.e., not all scenarios or hazards should be treated the same way with regards to DID. The IAEA guidance also explicitly discusses the relationship between PRA and DID, indicating that it is a "useful tool for optimizing efforts in implementing" DID; while also acknowledging that "some aspects of plant safety are difficult to assess quantitatively by probabilistic methods" and that this will most likely require deterministic plant design input.

A more recent IAEA document, IAEA SR-46 "Assessment of DID for NPPs" (issued in 2005) [7], provides a significant additional discussion on the topic of DID. It focuses on screening for DID aspects for an operating LWR NPP and proposes a systematic identification of the required safety provisions for the siting, design, construction and operation as a basis assessing the comprehensiveness and quality of DID at the NPP. Finally, the IAEA also published a report in 2016, IAEA TECDOC-1791 [8], that discusses how the IAEA safety requirements are to be considered in the design of NPPs. In this report, the IAEA DID Levels 1-5 are further split to account for the potential contribution of equipment used for Design Extension Conditions (DECs), i.e., conditions beyond the traditional Design Basis Accidents that may require some consideration (used in the regulatory structure of a number of countries). Two approaches to addressing the IAEA DID levels are provided to account for cases with or without significant fuel degradation/core melt. Their relationship to SM concepts is also included in this reference, with respect to Design Basis and DECs.

In addition, an European Commission-supported project was performed under the Advanced Safety Assessment Methodologies: Extended PSA (ASAMPSA_E) effort, coordinated by France's Institute for Radiological Protection and Nuclear Safety (IRSN), to investigate the use of PRA for DID purposes for NPPs [9]. The report documenting the investigation includes multiple international perspectives.
It supports the general concept that PRA information can and should be used for DID assessment in RIDM and it already contains a significant overlap in terms of considering the multiple DID layers and barriers (as well as supporting equipment and plant challenges that can impact DID). In particular, it states that risk insights from PRA models, if appropriately developed, "can provide a methodical support and an essential contribution for determining whether the safety objectives are met, the DID requirements are correctly taken into account". It also indicates that challenges exist in mapping DID deterministic concepts (e.g., design basis, safety-related/non-safety-related categories) to the general approach in PRA models and RIDM (e.g., best estimates as opposed to conservative design). The report recommends further investigation on "possible consensus about objectives, practical methodologies and scope" for assessing the use of risk insights and PRA in RIDM.

3. KEY CHARACTERISTICS TO CONSIDER FOR DID/SM IN RIDM

Based on some of the insights discussed in Section 2 (and a much wider literature review performed in EPRI 3002020763 [2]) a series of characteristics can be defined that, at a high level, are desirable for a framework in which to consider DID/SM in RIDM.

3.1 Integration of "Rationalist" and "Structuralist" perspectives on DID

While the more deterministic-minded, "structuralist" perspective was successful in adding a significant amount of DID capabilities in reactors, there has been enough operating experience to strongly suggest that vulnerabilities can filter through if a binary approach is taken (e.g., assuming an SSC that meets design requirements can never fail). It is also apparent that application of the purely deterministic approach has led to resource allocations in areas without significant risk benefits, which has since then been addressed through several decades of risk-informed changes to the licensing bases. Similarly, an approach to DID that only considers the physical barriers as the key DID layers ultimately fails to recognize the various elements (including programmatic aspects) that can support their function. This includes the complex system dependencies among the systems protecting the barriers and CCF events that can defeat system redundancy and fail them concurrently.

Hence, a key foundational element for a better formulation of a DID/SM framework in RIDM is one that incorporates the strengths of both the "structuralist" and "rationalist" perspectives, rather than promote one more heavily against the other. To this end, the approach in a seminal paper [10] on DID/SM (focused on the application of a framework to advanced reactor design) is used, as it provides a significant foundation in which to integrate both aspects. This approach includes the identification of the design, process, and scenario DID elements that capture both perspectives and indicates a path forward in which to incorporate key aspects of DID in a single framework.

3.2 Incorporation of Design, Programmatic, Scenario Aspects in DID/SM for RIDM

Often considered the cornerstone of the "structuralist" perspective, the design inputs into DID are a key aspect that must be considered whether DID is being assessed under a purely deterministic or RIDM perspective. This aspect of DID allows for design aspects focused more directly on the physical barriers (fuel cladding, RCS, containment) along with supporting components to be accounted for. Selection of materials and design aspects, including design variability in LWRs, can be directly incorporated in terms of how they support the overall DID protection.

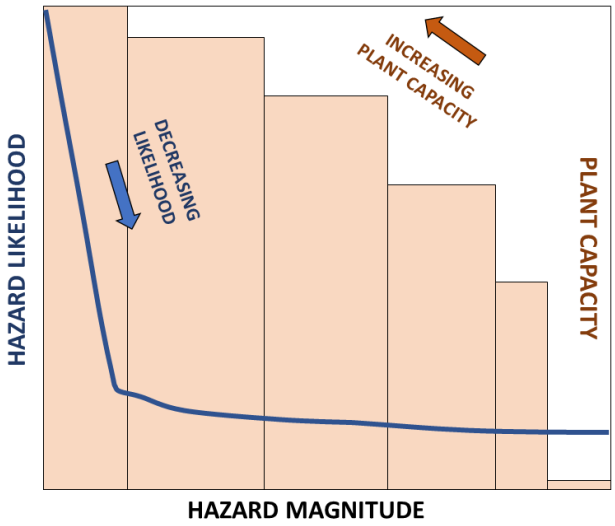
The DID perspectives that focus on design and/or physical barriers alone could omit the significant support that procedures, programs, and other processes built around the protection of the DID layers provides. While programmatic DID aspects are built around design DID aspects as well (e.g., via quality assurance programs), they are essential in the day-to-day assurance that DID protection is maintained during plant operations. Finally, there is an obvious feedback loop between programmatic DID and scenario DID in the sense that the reliabilities and capabilities of the SSCs reflected in the scenarios are significantly influenced by the contributions of programmatic aspects. Given the extensive presence of licensing and other regulatory issues in NPP aspects, it can be argued that programmatic DID has a strong element of supporting the RIDM principle of meeting regulatory requirements within the RIDM framework. This is yet another indication of how the individual RIDM principles should not be viewed in isolation.

Finally, the incorporation of risk assessments, where the distinction between design basis and beyond design basis is less relevant (if not irrelevant), provided a more graded perspective on how some accidents that were at some point considered "beyond" design basis could be indeed more frequent than certain DBEs (and, therefore, more important risk contributors). For example, certain beyond design basis can be identified as potentially more significant contributors, under certain conditions, due to operational events that involve CCFs exceeding the single failure criterion (e.g., station blackout, SBO, and anticipated transients without scram, ATWS). Therefore, some level of protection against them had to be considered, which caused the line between design basis and beyond design basis to became less clear. In addition, issues such as the balance between DID layers, independence between layers, redundance/diversity, and protection between CCF are much less clear cut when

considering different scenarios; which is why scenario aspects need to be carefully considered for DID/SM in RIDM.

Whether the hazard is a rupture of a large RCS pipe, a seismic event, or other IEs typically considered in licensing basis or risk assessment, the strength of DID does not remain constant at all levels of magnitude. There will be scenarios significant enough (e.g., a Large LOCA) where containment may be challenged. Similarly, for a natural hazard such as seismic events, there will be large but extremely unlikely ground motions levels for which a LOCA may occur (with a potentially concurrent structural damage of containment at even more extreme levels). A clear illustration of this aspect can be observed using the concept of hazards and the capability against the hazard (e.g., a conditional probability given a hazard level), typical in risk assessment, as illustrated in Figure 2.

Figure 2: Illustration of Scenario Specific Aspects for DID Purposes



3.3 Judicious Incorporation of Risk Insights

There is a significant incorporation of DID elements in the overall approach used in risk assessment, as exemplified by PRA models for NPPs. Ultimately, all approaches used for nuclear safety deal with the fundamental aspects of how accidents may evolve (regardless of design or other details). Whether deterministically or probabilistically, accident scenarios will consider various failures leading to the potential for multiple barriers to be impacted (either by direct failure of the barriers or bypass scenarios). They will also need to include emergency preparedness aspects (directly dependent on siting) and potential releases from possible hot core debris, radionuclides, and aerosols resulting in direct/indirect exposure paths.

The use of PRA information to better understand DID does not make the process “risk-based” as long as a strict interpretation of quantitative results is avoided, which is ultimately the overall intent of RIDM. However, it is also important to note that it is not a straight-forward exercise to understand how risk insights relate to DID. This requires a careful and judicious assessment of what DID elements are contained in PRA models, their relationship to DID levels, and what type of insights can be derived from the logic structure and quantitative risk results.

3.4 Adaptability to Different Interpretations of DID Levels

As mentioned in Section 2, there is not a single “correct” definition of DID or the elements, attributes, or characteristics that compose it. It is perfectly understandable that the complex phenomena and societal response associated with a reactor accident can be interpreted in various ways. Hence, discussing elements that could be applied more universally than typically discussed in any single country or regulatory environment is a highly relevant attribute.

3.5 Adaptability for Risk-Informed Applications

Different applications may require different interpretations of the purpose to assess DID and its implementation. For example, an application focused on the baseline risk will have a different perspective in terms of a plant licensing change, risk-informed technical specifications, low power and shutdown risk, and other applications. While for several cases the same essential process is performed using the PRA model (i.e., conditioning the risk assessment to a specific situation, either a component out of service or a specific plant operating state), how DID is viewed and interpreted can be significantly different. Hence, recognizing that different RIDM applications may result in different DID/SM implementation aspects (which can be interpreted differently depending on the application's context) is an important characteristic of any DID/SM consideration in RIDM. Without a clear framework, it is not necessarily straight-forward to assess such changes (since DID and risk results do not necessarily have a one-to-one correspondence). Hence, a proper framework that includes design and programmatic DID with practical use-oriented can go a long way to provide an integrated view of changes in risk as well as in DID that is adaptable to multiple RIDM applications.

3.6 Capability to Support both Qualitative and Quantitative DID Risk Insights

Multiple interpretations of DID include varying levels of qualitative and quantitative views of DID/SM. Including such an attribute is particularly important for areas where RIDM is not yet used but could be considered. As an example for discussion purposes, physical security at NPPs is an area where some risk insights are currently used, albeit not in the same manner as in quantitative-focused RIDM approaches, since there is a significant overlap between physical-security and the non-physical security element of DID (even if quantitative risk results are not always relied upon in physical security). Hence, ensuring that a framework accounts for different types of inputs could support its implementation not only on the more PRA results-focused areas but also to other applications where technical challenges exist to quantify all the individual inputs of the analysis.

3.7 Efficient Visualization and Communication for Practical Use

One of the most challenging aspects in discussing DID/SM in general is the level of complexity and inter-connectedness that these principles contain. While it is less challenging to visualize the typical physical barriers associated with DID (which is why they can be often be interpreted as the narrower understanding of the DID concept itself), it is more difficult to visualize how individual SSCs as well as non-physical (but no less important) aspects such as programmatic and risk inputs relate to the concept. As described in EPRI 3002014783 [1] (see Appendix E in that report), visualization and communication of insights from RIDM tends to be an on-going challenge in certain areas (e.g., communicating risk insights with non-risk experts). Hence, an approach that is not focused purely on risk outputs or overarching risk results can provide a bridge between the risk expert and the non-risk expert to the benefit of the entire NPP organization involved in nuclear safety.

4. A FRAMEWORK FOR CONSIDERATION OF DID/SM IN RIDM

Based on the characteristics discussed in Section 3, a general framework for the consideration of DID/SM in RIDM is developed, which is intended to be flexible for an individual issue or hazard as well as for an overarching review of the effectiveness of the DID implementation at an NPP. The framework is developed in part based on the overall process described in a paper [10] by Fleming and Silady. The framework includes a high-level approach to the inclusion of design, programmatic, and scenario DID aspects as follows:

- Establishment of an alignment with DID philosophy definitions and describing how multiple layers of defense can be deployed to confirm DID adequacy,
- Description of how protective DID strategies are used to define the DID attributes incorporated into plant capabilities that support each layer of defense (where the resolution of general

protective strategy concepts into sets of DID attributes is made to support the objective evaluation of DID adequacy)

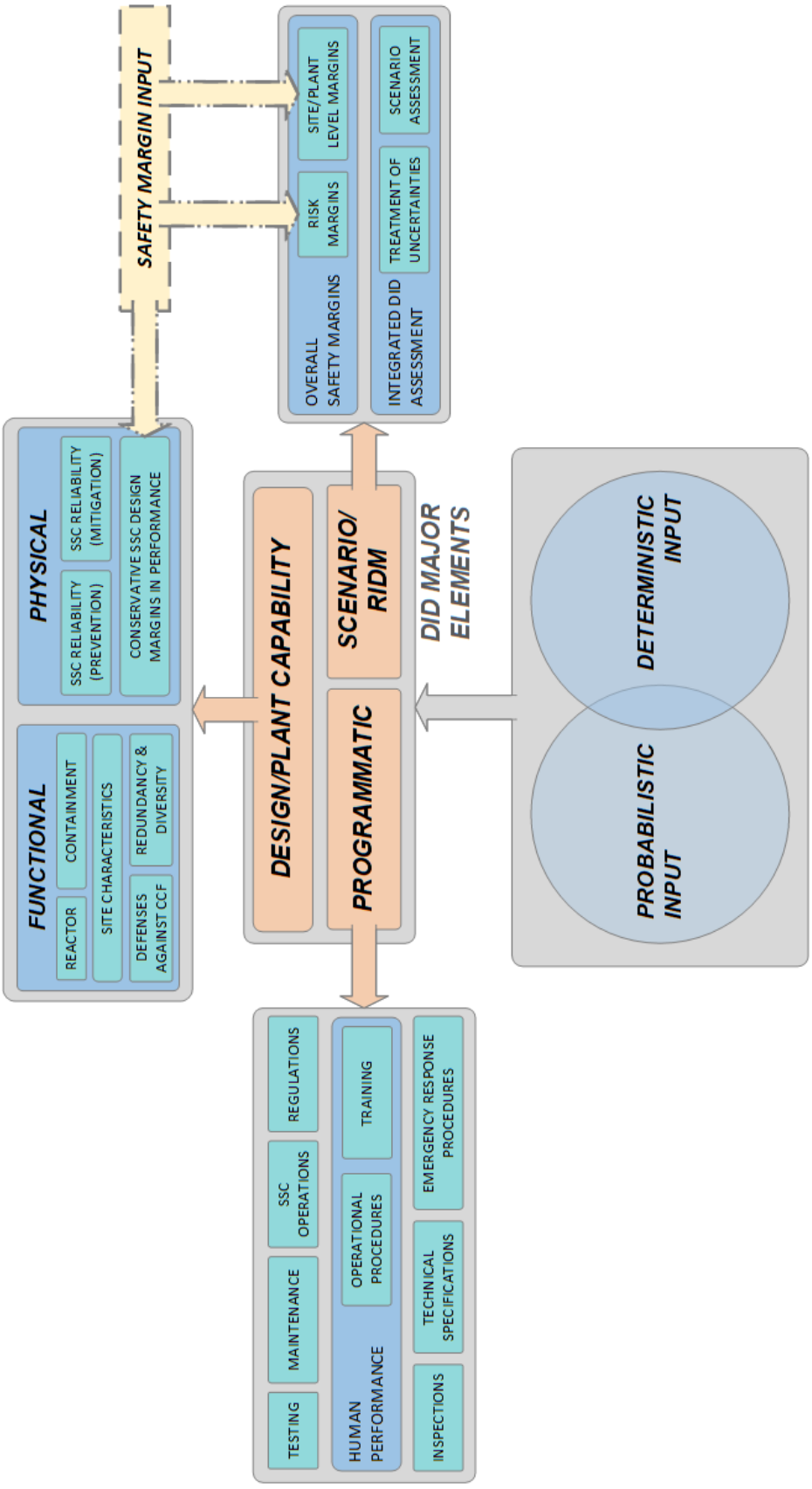
- Incorporation of DID attributes reflected in plant design features, reliabilities, and capabilities of SSCs that include fission-product barriers contributing multiple, functionally independent layers of defense in the prevention and mitigation of accidents,
- Summary of programmatic attributes of DID to provide assurances that DID plant design capabilities are realized,
- Discussion of the role of programmatic DID attributes to compensate for uncertainties, human errors, and hardware failures,
- Identification of the importance of defense against CCF and the need to minimize dependencies among layers of defense, and
- Presentation of guidelines for evaluating DID adequacy.

A high-level illustration of the overall approach is shown in Figure 3, which also highlights how SM fits within a general DID approach, with SSC-level SMs and plant-level SMs (including risk and deterministic margins); highlighting a clearer link between DID and SM than current guidance establishes. Note that extensive details on the framework, its relationship to the key attributes in Section 2, and the specific inputs for each individual aspects are discussed in EPRI 3002020763 [2].

Within this framework, assessing DID/SM in RIDM is not taken as an exercise in obtaining quantitative risk results (this would be a risk-based approach), but as a balanced approach to risk-informing the assessment. The distinction of prevention/mitigation can be arbitrary as it is highly dependent of on the point of reference used. In this respect, the DID/SM capability can be assessed against core damage, releases into containment, releases outside containment, up to and including progression of offsite doses. Similarly, the scope and level of use of the DID/SM framework discussed here can be assessed up to the individual points typically used to delineate the PRA Levels (i.e., 1, 2, 3). Depending on the scope of the analysis and availability of resources, a full scope, all hazards, all POSs PRA model is not a requirement if the scope is to assess DID/SM against core damage and/or large releases (the level of granularity with respect to PRA Level 2 and 3, however, will not be available in this case). This effort does not envision a strict requirement to perform a full PRA Level 3 to be able to take advantage of this work. In fact, since qualitative information can be used, assumptions of releases and offsite dose consequences can be linked to the Level 1/2 information as needed (i.e., emergency preparedness is still a DID level to be accounted for, whether a detailed Level 3 PRA is performed or not).

As discussed in the paper [10] by Fleming and Silady, PRA models include accident sequences that could have various interpretations regarding the delineation of prevention versus mitigation, given that they generally include:

Figure 3: A Framework for Consideration of DID/SM in RIDM



- An initiating event that constitutes a challenge to the plant SSCs responsible for control of transients and protection of the plant SSCs (including the radionuclide transport barriers),

  - Some PRA models include explicit logic structures for contributors to IEs (defined as support system initiating events) that can provide insights into potentially important dependencies.

- The response (successes and failures) of plant SSCs 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,
- The response of each barrier to radionuclide transport from the radioactivity sources to the environment to the IEs and safety system responses,
  - This response is expressed as the degree of retention of radioactive material for each barrier expected for the sequence (i.e., fuel elements, RCS, containment).
- The implementation of emergency plan protective actions to mitigate the radiological consequences of a given release from the plant.

In EPRI 3002020763 [2], a detailed discussion of how aspects of DID/SM for individual hazards (internal and external) in RIDM can be based on the accident sequence level with a potential quantification based on prevention and mitigation definitions is presented; along with how risk metrics can be considered within DID/SM aspects. For brevity purposes, this will not be repeated here. Instead, an example is discussed next to highlight a practical implementation of the approach.

5. IMPLEMENTATION OF THE FRAMEWORK USING PRA INFORMATION

In order to illustrate the application of the DID and SM evaluation in RIDM discussed in Section 4, example applications are presented in this section. The examples are based on the PRA model of an operating U.S. NPP which is used in multiple risk-informed regulations. In other words, the PRA model has been technically peer-reviewed and its results have formed the basis for regulatory submittals that have been accepted for implementation (i.e., it is a representative of an advanced state-of-practice risk model for its purposes). The PRA model is based on a PWR design (Westinghouse Four-Loop) with a large dry, ambient pressure containment. The specific site of the NPP includes two-reactors of the same design (dual-unit site). It should be noted that the PRA model documentation for this NPP is extensive, and includes PRA Level 1 modeling of internal events (see Figure 4), internal fire, internal flood, and seismic events. It also includes a PRA Level 2 model that can calculate the frequency of both large early releases (LERF) and small early releases (SERF).

Figure 4: Internal Events Initiating Event Frequency vs. Conditional Core Damage Probability

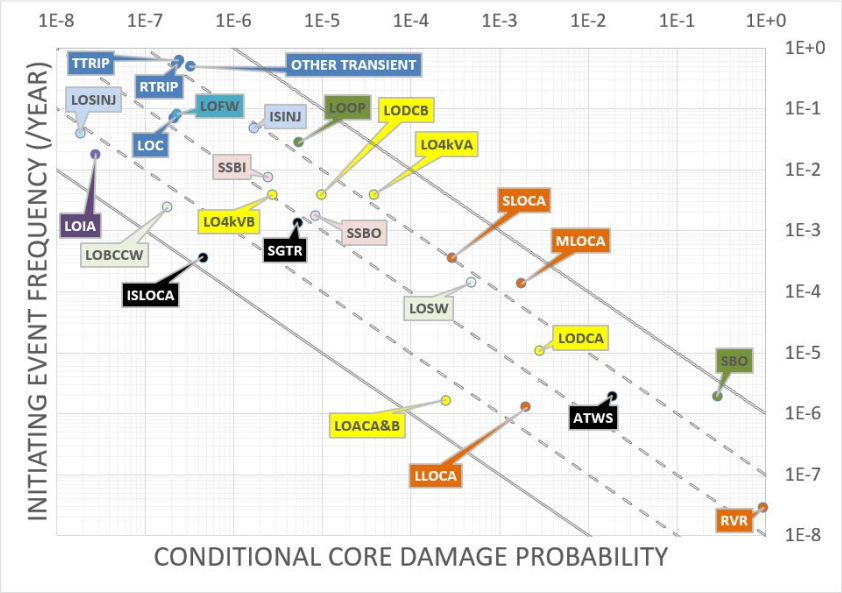


Figure 4, although high level, allows the visual assessment of the balance between the IE frequency (and, to some extent, prevention, in cases where the IE was modeled as a fault tree), as well as the corresponding capability of the plant to prevent core damage (conditioned on the event occurring). Insights regarding DID may be gained from examining the contributions to CDF, LERF, and CLERP from individual IEs. Of the modelled IEs, about 15 account for more than 95% of the CDF (and a similar number for LERF) for the internal events. It is noteworthy that all but 5 of the 26 modelled IEs have a CLERP value lower than 3.1×10^{-3}. Upon examination of the major contributors to LERF, it is seen that the 5 IEs that have higher CLERP all involve containment bypass from containment isolation failure or containment bypass due to ISLOCA, un-isolated SGTR, induced SGTR, or RCP seal LOCA with un-isolated seal return line. The IEs with the lower CLERP values do not have significant containment bypass contributions and the dominant contributor to containment failure for those IEs appears to be un-isolated and pre-existing leaks or tears in the containment barrier. The containment event tree split fraction for this failure mode is 1.1×10^{-3} which makes up most of the CLERP values for these IEs. An important DID insight from the review of the LERF contributions is that containment failures due to severe accident phenomena such as steam explosions, direct containment heating, hydrogen combustion, and other high pressure melt ejection phenomena make insignificant contributions to LERF for the internal events hazard group. From the internal events PRA model, there are four sequences defining unique end states in the Level 2 PRA results that comprise more than 99% of LERF for the internal events at full power hazard group.

In this PRA model, Medium LOCA produces the top-ranking accident sequence cutset for non-SBO results. An analysis of Medium LOCA sequences shows a cutset of interest for exercising the DID/SM framework of Section 3 further with respect to the use of risk insights. The path through the Level 1 PRA event tree for Medium LOCA involves successful High-Pressure Injection and failure to establish High-Pressure Recirculation leading to the Level 1 end state "MLOCA". In the Level 2 PRA event tree there is successful prevention of a containment bypass and then failure to isolate containment due to pre-existing leaks resulting in the Level 2 PRA end state with LERF 1. The remaining risk significant accident sequence cutsets for LERF 1 have different pathways through the Level 1 PRA event trees from non-SBO IEs but take the same path through the Level 2 PRA event tree with LERF due to containment isolation failure. This investigation provides a useful way to examine the DID principle of balancing the prevention and mitigation of accident sequences and the identification of the plant design features responsible for this balance (shown in Figure 5).

Figure 5: Evaluation of Prevention/Mitigation for a Medium LOCA Accident Sequence

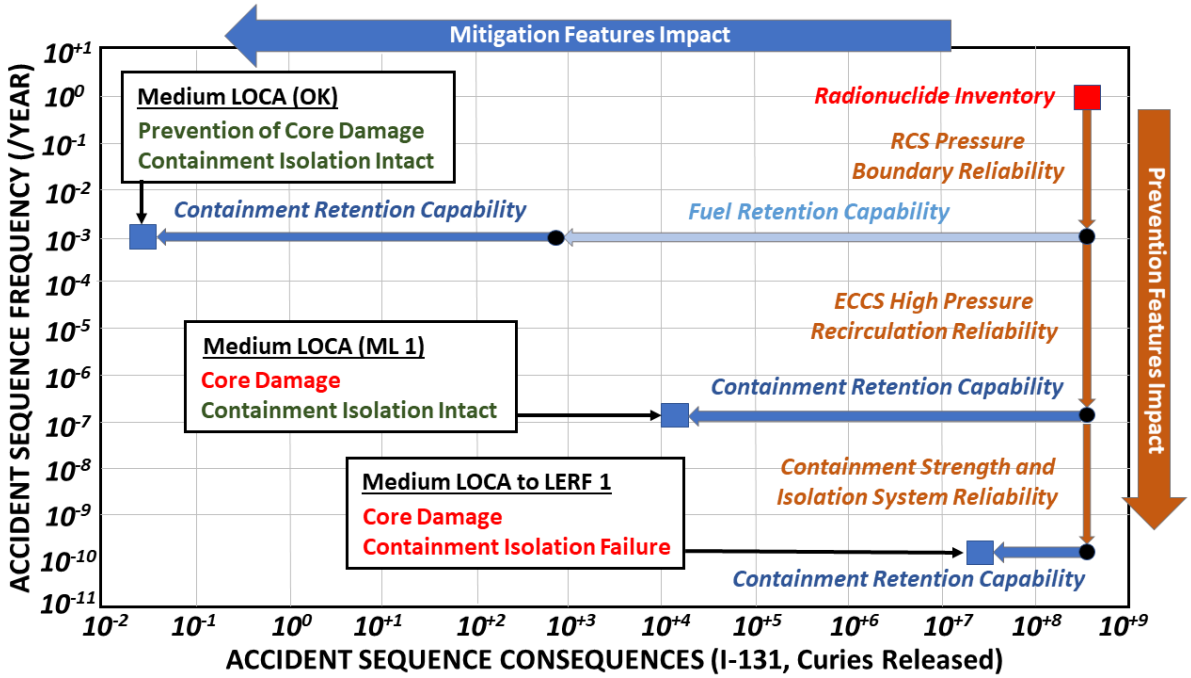


Figure 5 uses the PRA model results coupled with generic PWR source term release fractions for I-131 available from the U.S. NRC State of the Art Consequence Analysis (SOARCA) results (for example, in NUREG-1935 [11]), as surrogates for Level 3 PRA results. Figure 5 starts with the certainty of the I-131 radionuclide inventory in the upper left-hand corner of the frequency versus consequence plot. The down arrows reflect the design features responsible for first preventing the IE, second for preventing core damage, and third for preventing a large early release. The horizontal arrows reflect the mitigation of the source term associated with retention in the fuel for the non-core damage sequence and retention in the containment for all three sequences.

In EPRI 3002020763 [2], this is one of several sequences studied using the framework; others include multiple Medium LOCA cutsets, SGTR sequences. internal fire and flood sequences, and seismic events. The input from these insights can be further coupled with the information needed as input to Figure 3, in terms of design, programmatic, and scenario DID inputs in addition to further leveraging of PRA modelling information such as contributors to common cause failures (CCF), operator actions, and other elements relevant to the overall framework.

4. CONCLUSION

From an extensive literature review, DID/SM in RIDM are overdue for a better, more efficient manner of addressing both specific topics in RIDM principles, as well as general issues related to uncertainty, completeness, and comparison against risk criteria. Through the framework presented here (or, at least, through several of the elements presented here), this can be accomplished in a way that benefits RIDM implementation in general, while informing both risk experts and non-risk experts. Future activities will be focused on developing an assessment of DID/SM that is more complete in terms of linking design/programmatic aspects further with insights from scenario DID to evaluate the baseline DID/SM posture of an individual plant/site as well as with respect to risk-informed application(s) of interest.

References

[1] Electric Power Research Institute. *"A Framework for Using Risk Insights in Integrated Risk-Informed Decision-Making"*. Palo Alto, CA: 2019. 3002014783.

[2] Electric Power Research Institute. *"Consideration of Defense-in-Depth and Safety Margins in Risk Informed Decision Making: Practical Guidance"*. Palo Alto, CA: 2021. 3002020763.

[3] U.S. Nuclear Regulatory Commission. "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis. Regulatory Guide 1.174", Revision 3, January 2018.

[4] U.S. Nuclear Regulatory Commission. *"Historical Review and Observations of Defense-in-Depth*". NUREG/KM-0009, April 2016

[5] J. N. Sorensen, G. E. Apostolakis, T. S. Kress, and D. A. Powers. *"On the role of defense in depth in risk-informed regulation."* International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 1999), Washington, DC (August 1999).

[6] International Atomic Energy Agency. *"Defence In Depth in Nuclear Safety"*. INSAG-10 Report, January 1996.

[7] International Atomic Energy Agency. *"Assessment of Defence In Depth in Nuclear Safety"*. Safety Report No. 46, February 2005.

[8] International Atomic Energy Agency. *"Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants."* TECDOC Report 1791, May 2016.

[9] European Commission. *"The Link between the Defence-in-Depth Concept and Extended PSA*." Report ASAMPSA_E / WP30/ D30.7/2017-31, Volume 4, December 2016.

[10] K. N. Fleming, and F. A. Silady, *"A Risk Informed DID Framework for Existing and Advanced Reactors"* Reliability Engineering & System Safety, Vol. 78, No. 3, p. 205 (2002).

[11] U.S. Nuclear Regulatory Commission. *"State-of-the-Art Reactor Consequence Analyses (SOARCA) Report"*. NUREG-1935, Volume 1, November 2012.