Nuclear Engineering and Design 330 (2018) 157–165

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

Integrating quantitative defense-in-depth metrics into new reactor designs☆

Cindy Williams*, William J. Galyean, Kent B. Welter

NuScale Power, LLC, 1100 NE Circle Blvd., Suite 200, Corvallis, OR 97330 United States

ARTICLE INFO

Keywords:
Defense-in-depth
Risk-informed
Performance-based
PRA
Reactor
Design

ABSTRACT

Risk-informed, performance-based (RIPB) methods have progressed to the point where high-level guidance can be used to augment traditional, deterministic, nuclear safety design practices in areas important to nuclear reactor safety. This paper describes an approach for augmenting the traditional defense-in-depth (DID) qualitative approach with quantitative risk information from a plant-specific probabilistic risk assessment (PRA) in a way that is structured, can be applied on a consistent basis, and allows for clear acceptance criteria. Adding performance-based targets that should be achieved is expected to result in safer and more economical plant designs. Evaluations of DID can be conducted throughout the design process as well as in support of design certification and operating license applications to identify where defense protections could be enhanced or relaxed. Consistent with the United States Nuclear Regulatory Commission's policy statement encouraging greater use of PRA to improve safety decision making and regulatory efficiency, this scenario-based DID method can be used to evaluate changes and overall plant design as part of the normal design control process. Although the RIPB method presented in this paper was developed for application to advanced passive light water reactor designs, the metrics could be tailored to other reactor designs. This risk-informed approach to DID helps to ensure that public and worker risk insights are integrated into the design process holistically.

1. Introduction

Nuclear power plants must be designed to generate electricity in a safe, reliable, and economical manner. Design processes for existing light water reactors (LWRs) have relied heavily on deterministic design methods and deterministic analyses to ensure safety and comply with regulatory requirements. Risk evaluations have typically been performed after a significant amount of design work has been completed to ensure compliance with United States (U.S.) Nuclear Regulatory Commission (NRC) safety goals. These risk evaluations support, in part, qualitative and deterministic defense-in-depth (DID) assessments. Defense-in-depth is a design philosophy aimed at ensuring safety is not dependent on any one feature; it employs successive levels of redundant and diverse safety functions in design, construction, and operation to ensure appropriate barriers, controls, and personnel are in place to prevent, contain, and mitigate accidents and exposure to radioactive material. This philosophy has evolved over the history of nuclear power plant design with the overall goal of ensuring adequate safety to the public. The purpose of this paper is to outline an approach for a more quantitative assessment of the effectiveness of the implementation of the DID design philosophy.

Implementing the philosophy of DID includes a broad set of integrated design processes. They address accident prevention, accident mitigation, and risk management. Reactor design DID, as described here, consists of the integration of three strategies:

1. The first strategy employs conservative codes, standards, and analysis methods in the design to ensure margins of safety exist so as to minimize potential impacts of uncertainty. Multiple and successive barriers are employed to prevent, contain, and mitigate exposure to an accidental fission product release.
2. The second strategy involves programs and processes that serve to ensure fission product barrier function is designed with appropriate reliability and maintained throughout the life of the plant.
3. The third strategy requires evaluating the effectiveness of these fission product barriers to maintain their effectiveness and

☆ *Funding:* This material is based upon work supported by the Department of Energy under Award Number DE-NE0000633, an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

* Corresponding author.
E-mail address: cwilliams01@nuscalepower.com (C. Williams).

https://doi.org/10.1016/j.nucengdes.2018.01.008
Received 7 September 2017; Received in revised form 29 December 2017; Accepted 2 January 2018

reliability to ensure they continue to perform their design safety functions under abnormal conditions.

While the general design criteria in 10 CFR 50 are the key inputs into the requirements analysis process from a regulatory perspective, alternate or additional requirements may be needed for new and advanced reactors in cases of unique technologies, designs, or site characteristics (U.S. Code of Federal Regulations, 2015a). While there are numerous ways in which to integrate risk-informed, performance-based (RIPB) principles and methods into the design process (e.g., reliability assurance program), this paper describes the method by which an RIPB approach is being used within existing NRC guidance to augment the traditional DID philosophy for advanced passive LWRs.

Although traditional nuclear power plant design was based on deterministic and conservative analysis techniques, the results did not guarantee a conservative design. Advancements in probabilistic risk assessment (PRA) methods have led to their use in improving plant design and operations. Because PRAs realistically reflect actual plant design, construction, operational practices, and operational experience, they have proven to be a valuable complement to traditional engineering approaches. Use of PRA in regulatory matters to the extent supported by state of the art methods and data has resulted in measurable improvements in nuclear reactor safety by reducing the likelihood and consequences of potential severe accidents.

The proposed approach describes a method for augmenting the traditional DID philosophy with risk information from the PRA that is structured, quantifiable, and can be applied on a consistent basis; this approach reduces subjectivity and supports risk-informed decision making. Metrics are proposed to evaluate the adequacy of DID, which can be used to: (1) establish a DID baseline for the plant, and (2) serve as a method for evaluating the adequacy of DID in design changes. While integration of RIPB principles and methods are most effective early in the design process when risk insights can be used to support early trade studies and decision making, caution should be taken since early versions of the PRA have larger uncertainties due to the lack of design detail. Evaluations of plant DID can be conducted throughout the design development process as well as in support of design certification and operating license applications.

Although the metrics proposed here are intended for use on advanced passive LWR designs, it is expected that they can be tailored to other, technology-specific reactor designs that use similar metrics for evaluating plant risk such as core damage frequency and large release frequency. This risk-informed DID approach allows incorporation of risk insights early, and more broadly, into the design process holistically; it can be used to help ensure the design, construction, and operation of a new reactor design poses no undue risk to the health and safety of the public.

2. Defense-in-depth

The concept of DID is a longstanding principle used in the evaluation of nuclear plant licensing. While somewhat different definitions have been used in various regulatory documents, the definitions consistently include the concept that implementation of DID helps assure plant safety by providing barriers to radionuclide release such that safety is not dependent on a single barrier. The current definition of DID in the NRC glossary is:

> *An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.*

The concept of DID has further been used to account for uncertainties in safety analyses; the extent to which DID is applied can be determined, in part, by the use of risk insights (U.S. Nuclear Regulatory Commission, 2016):

> *The concept of defense-in-depth has always been and will continue to be a fundamental tenet of regulatory practice in the nuclear field, particularly regarding nuclear facilities. Risk insights can make the elements of defense-in-depth more clear by quantifying them to the extent practicable. Although the uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense makes regulatory sense. Decisions on the adequacy of or the necessity for elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance.*

While it is widely accepted that DID helps to ensure safe LWR operation, at the same time, it is recognized that DID is challenging to measure or quantify because philosophies differ (U.S. Nuclear Regulatory Commission, 2016). Incorporation of risk insights can be formalized in an RIPB approach to DID, and by extension, to plant design; this is consistent with the NRC policy statement on the use of PRA (U.S. Nuclear Regulatory Commission, 1985):

> *The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that compliments the NRC's deterministic approach and supports the NRC's traditional DID philosophy.*

2.1. Defense-in-depth regulatory requirements

Defense-in-depth has been at the core of the NRC's safety philosophy, and remains fundamental to the safety and security expectations of NRC's regulatory structure. The following summarizes key regulatory documents with regards to DID and risk-informed decision making to nuclear power licensing:

- 10 CFR 100.1(d), Reactor Site Criteria: states that DID be considered in reactor siting criteria (U.S. Code of Federal Regulations, 2015b).
- Policy Statement on the Regulation of Advanced Reactors: sets expectation that designs incorporate the DID philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents (U.S. Nuclear Regulatory Commission, 2008).
- Standard Review Plan Section 19.0, Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors: recommends that applicants identify risk-informed safety insights based on systematic evaluations of risk such that the design's robustness, levels of DID, and tolerance of severe accidents initiated by either internal or external hazards can be evaluated (U.S. Nuclear Regulatory Commission, 2014).
- NUREG-2150, A Proposed Risk Management Regulatory Framework: observes that, "there is no guidance on how much DID is sufficient," and that risk assessment, in combination with other technical analyses, can inform decisions about appropriate DID measures (U.S. Nuclear Regulatory Commission, 2012).
- Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis: provides the framework for current licensing decision making, establishes that DID should be maintained to address uncertainties, and encourages the use of risk analysis to provide insights on the "extent of defense-in-depth" (U.S. Nuclear Regulatory Commission, 2011).

2.2. Objectives of defense-in-depth within a risk-informed and performance-based framework

The inclusion of RIPB elements into the philosophy of DID provides