A Framework for Regulatory Requirements and Industry Standards for New Nuclear Power Plants*

Felicia A. Durán and Allen L. Camp
Sandia National Laboratories, P.O. Box 5800, MS 0747, Albuquerque, NM 87185-0747, United States
faduran@sandia.gov, alcamp@sandia.gov
George Apostolakis and Michael Golay
Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, United States
apostola@mit.edu, golay@mit.edu

Abstract

This paper summarizes the development of a framework for risk-based regulation and design for new nuclear power plants. Probabilistic risk assessment methods and a rationalist approach to defense in depth are used to develop a framework that can be applied to identify systematically the regulations and standards required to maintain the desired level of safety and reliability. By implementing such a framework, it is expected that the resulting body of requirements will provide a regulatory environment that will ensure protection of the public, will eliminate the burden of requirements that do not contribute significantly to safety, and thereby will improve the market competitiveness of new plants.

1. Introduction

Current regulatory requirements and industry standards for nuclear power plants (NPPs) are a collection of deterministic criteria, based largely on engineering judgement, that have evolved over the last 40 years. A growing awareness within government and industry is that many of the current requirements are not contributing significantly to safety and, therefore, have driven costs of new NPPs into a range that will not be economically competitive in a deregulated electric power industry.

The state of the art of probabilistic risk assessment (PRA) is sufficiently mature that we can apply PRA to identify systematically the requirements needed to maintain a desired level of safety. The U.S. nuclear industry and the U.S. Nu-

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

DISCLAIMER

clear Regulatory Commission (NRC) are already working together to apply risk-informed regulation to the regulation of existing plants [1]. The NRC/industry efforts are progressing to address primarily the operation and maintenance of existing plants. Of course, this effort is constrained by the fact that the operating plants have been licensed under the traditional regulatory system. What is needed beyond the current effort is a new approach to all requirements, focusing on the design and licensing of future plants. This paper summarizes the development of a framework for risk-based regulation and design for new NPPs.

2. Structuralist vs Rationalist Approach to Defense in Depth

Current regulations and standards are based, in large part, on the principles of defense in depth (DID) and safety margins, which have evolved since the first reactors were designed in the 1940s. The NRC Advisory Committee on Reactor Safeguards (ACRS) [2] and Sorensen et al. [3] discuss this evolution, identify two schools of thought on DID, labeled "structuralist" and "rationalist," and recommend an approach for risk-informed regulation.

The structuralist view asserts that DID is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. In contrast, the rationalist view asserts that DID is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression.

The two views are not necessarily in conflict. Both can be considered as a way of dealing with uncertainty. Neither incorporates an absolute means to determine when the degree of DID achieved is sufficient. The main difference is that the structuralist accepts DID as a fundamental principle, while the rationalist would place DID in a subsidiary role. Additionally, the structuralist does not deal with uncertainties in a quantitative manner, while the rationalist takes advantage of the fact that advances in PRA allow the quantitative estimation of some of these uncertainties. For new plants, the rationalist approach to DID, employed within the context of PRA, is preferred to more effectively develop a body of regulations that eliminates requirements that do not contribute significantly to safety.

The rationalist relies on PRA techniques to provide an integrated and systematic analysis of the plant that explicitly addresses sources of uncertainty. The process envisioned by the rationalist is: establish quantitative safety goals, such as the health objectives, core damage frequency, and large release frequency; design and analyze the plant using PRA methods to establish that the safety goals are met; evaluate the uncertainties in the analysis, including those due to model in-

adequacies, system performance and reliability, and lack of knowledge; and determine what steps (i.e., DID, new design features) to take to address those uncertainties. The quantification of uncertainties provides a means for determining how much redundancy and diversity (i.e., DID) is sufficient.

3. Development of the Framework

The framework, illustrated in Figure 1, is being developed using a top-down hierarchy, indicated on the left side of Figure 1, to define the goal, establish an overall approach, and develop and implement appropriate strategies and tactics. The framework is based on an application of PRA methods and reflects a rationalist approach to DID.

The principal *goal* of regulations for NPPs is to ensure adequate protection to the health and safety of the public. The NRC has established safety goals including Quantitative Health Objectives (QHOs) that state the Commission's expectations with respect to how safe is safe enough. Although the NRC's safety goals are not considered quantitative measures of adequate protection, for new plants, we will consider the determination of adequate protection using increased reliance on comparisons of PRA results to quantitative risk measures. The goals we are using for this framework, have been adapted from the NRC's goals and are indicated in the gray boxes in Figure 1.

The general *approach* for this framework is to evaluate risk against quantitative safety goals. High confidence is achieved through explicit consideration of uncertainties, including modeling adequacy and equipment design and performance, in a full-scope, detailed PRA for all operating modes. The primary *strategy* for both developing and evaluating compliance with requirements for risk-based regulation and design is to use PRA to quantify risk and uncertainties. This strategy provides a mechanism for integrating the risk information available from Level 1, Level 2, and Level 3 PRA analyses. A Level 1 PRA evaluates the potential for accident initiators and the system response to prevent core damage. An estimate of core damage frequency is compared to the corresponding goal. A Level 2 PRA encompasses the response and mitigation of core damage, including containment of fission products. The risk estimates here can be compared to goals for conditional probability of large release, both early and late. A Level 3 PRA encompasses the response and mitigation of radionuclide releases, including emergency response. These risk estimates can be directly compared to the QHOs or to subsidiary goals for conditional probability of early fatalities and latent cancer risks.

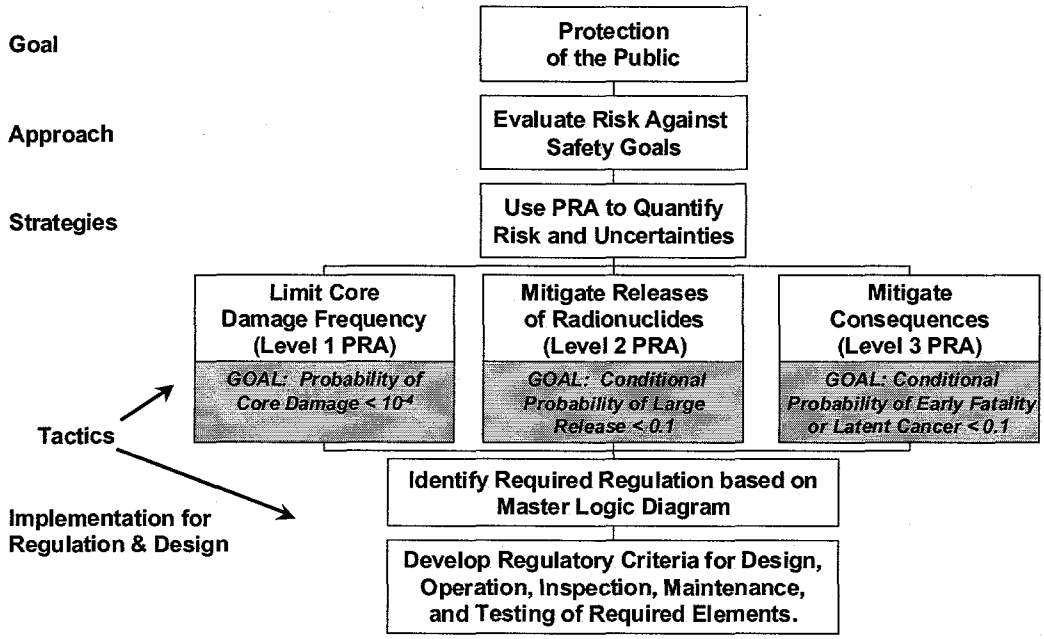

Figure 1 Framework for risk-based regulation and design.

To develop risk-based regulations, *implementation* of the framework is achieved by defining functional system characteristics, within the context of how PRA is performed, to determine what areas need to be regulated to assure safety. Implementation for design is achieved by specifying design configurations and using PRA to evaluate the design, then iterating with subsequent design changes. A master logic diagram (MLD), illustrated in Figure 2, is used to take a top-down approach to identify the safety functions, and systems, structures, and components (SSCs) that are required to maintain safety and to identify the accident initiators and system response failures that could compromise safety [4]. The top event is stated in terms of risk exceeding the safety goals. The gray shaded events correspond to Level 1, Level 2, and Level 3 PRA strategies, respectively, in Figure 1. The sixth level of the MLD defines the system functions that are required to assure safety. The next level down indicates that initiating events and failure of mitigating systems, containment, and emergency response can compromise safety functions. The last level of the MLD indicates that internal initiators for all operating modes and external initiators will be considered for completeness. Further development of the MLD will determine the "regulatory risk space" for which regulatory and design requirements are needed.

Various *tactics* (e.g., design criteria, procedures, redundancy, emergency response, etc.) are applied to support the PRA strategies and implementation. Once the SSCs required to achieve safety have been identified, then decisions on appro-

priate tactics for regulation and design can be made. The specification of these tactics will be based on a systematic evaluation of the areas that need to be regulated for the purposes of assuring safety and will also evolve from this process.

4. Summary

We have presented a framework for risk-based regulation and design for new NPPs. PRA methods and a rationalist approach to DID are used to develop the framework. For new plants, a detailed plant-specific PRA for all operating modes, along with an explicit treatment of uncertainties, would confirm that established quantitative safety goals are met. Within the current capabilities of PRA methods, sources of uncertainty will be quantified to gain as complete an understanding as possible about the range of risk and uncertainty before DID is applied to address uncertainties. Within this framework, PRA provides the basis for both developing and evaluating compliance with requirements for risk-based regulation and design.

5. References

1. U.S. Nuclear Regulatory Commission, Framework for Risk-Informing Regulations, Draft for Public Comment, Rev. 1.0, February 10, 2000, http://nrc-part50.sandia.gov/Document/framework_(4_21_2000).pdf
2. Letter to Shirley Ann Jackson, Chairman, U.S. Nuclear Regulatory Commission, from D.A. Powers, Chairman, Advisory Committee on Reactor Safeguards, Subject: The Role of Defense in Depth in a Risk-Informed Regulatory System, May 19, 1999
3. Sorensen, J.N., Apostolakis, G.E., Kress, T.S., and Powers D.A., On the Role of Defense in Depth in Risk-Informed Regulation. Proceedings of The International Topical Meeting on Probabilistic Safety Assessment, Washington, DC, pp. 408-413, 1999
4. Apostolakis, G.E., Some Issues Related to Goal Allocation and Performance Criteria. Proceedings of the 8th International Conference on Structural Mechanics in Reactor Technology, Brussels, Belgium, Paper M2 4/3, 1985

Acknowledgement: This work was performed as part of the U.S. Department of Energy's (DOE's) Nuclear Energy Research Initiative (NERI).

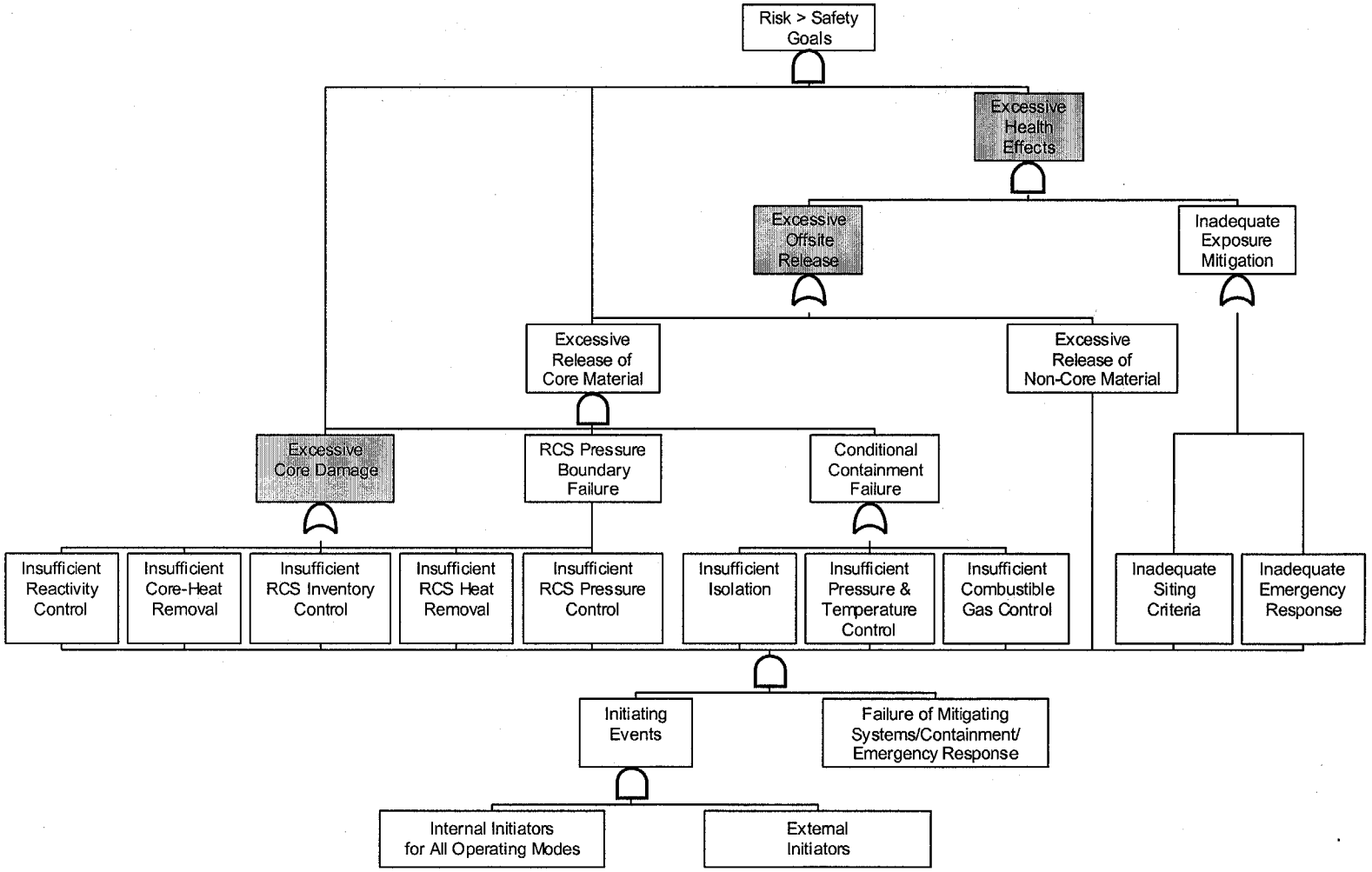

Figure 2. Example master logic diagram for framework implementation.