Reliability Engineering and System Safety 95 (2010) 935–943

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Use of risk measures in design and licensing of future reactors

Kamiar Jamali

United States Department of Energy, Office of Nuclear Energy, 1000 Independence Avenue, Washington, DC 20585, USA

ARTICLE INFO

Article history:
Received 17 February 2010
Received in revised form
5 April 2010
Accepted 6 April 2010
Available online 10 April 2010

Keywords:
Nuclear reactor safety
Probabilistic risk assessment (PRA)
Safety goals
Acceptance criteria
Next generation nuclear plant
Small modular reactors
Frequency-consequence curve

ABSTRACT

Use of information and insights from probabilistic risk assessments (PRAs) in nuclear reactor safety applications has been increasing by the nuclear industry and the regulators, both domestically and internationally. This is a desirable trend, as PRAs have demonstrated capability to improve safety and operational flexibility beyond that provided through deterministic approaches alone. But there can be potential pitfalls. The limitations of risk assessment technology can be lost through approaches that rely heavily on quantitative PRA results (referred to as risk measures in this paper), because of the unambiguous but potentially misleading message that can be delivered by risk-based numbers. This is particularly true for future reactors, where PRAs are used during the design and licensing processes. For these applications, it is important to ensure that the actual, de facto, or even perceived use of risk measures in the context of either regulatory or design acceptance criteria is avoided. While the issues discussed here can have a significant influence on design certification or combined license applications for future reactors, they can also have secondary impacts on currently operating reactors.

Published by Elsevier Ltd.

1. Introduction

Probabilistic risk assessment (PRA) results and insights have helped to improve nuclear power plant safety and operational flexibility for more than 30 years. This success has led to increased use of PRAs by the nuclear industry and regulatory authorities worldwide. While this trend is largely positive, there can be potential negative consequences that have not been widely discussed in related literature, with some exceptions (e.g., [1]).

It was because of this positive contribution to safety that the US Nuclear Regulatory Commission (NRC) gradually refined their original deterministic-based nuclear safety regulations by incorporating the use of risk information and insights within a risk-informed framework. Risk-informed regulations for the current fleet of operating light-water reactors (LWRs) are defined through a combination of rule-making and publication of lower-tier documents, such as regulatory guides or NRC's endorsement of certain nuclear industry documents. Thus, in a risk-informed framework, risk information and insights supplement the traditional deterministic approaches and form a part of the overall safety case (which is sometimes referred to as the safety basis) for a nuclear plant. The Commission has also called for increased use of PRA technology in all regulatory matters in a manner that complements NRC's predominantly deterministic approaches within the confines of a risk-informed as opposed to a risk-based regulatory construct. Some of the distinguishing features between the two are also discussed in this paper.

The nuclear industry also has used PRA techniques extensively with beneficial results, including in the design of advanced or evolutionary nuclear reactors. These benefits are, in part, related to the fact that these same users can also control and limit the influence of the incomplete safety information that is provided through the results of the PRA alone. Factors that are usually not fully accounted for in a PRA model but are germane to the consideration of adequacy of safety features for a specific issue or accident scenario may include: magnitudes of relevant safety margins, incorporation of defense in depth, potential for corrective or compensatory actions, degree of conservatism in analysis, and many others. The very same PRA information, however, when used to comply with well-intentioned regulatory policies and approaches can lead to some undesirable consequences. Some of the undesirable consequences in applications involving future reactors are also discussed below.

PRAs provide both qualitative and quantitative information. Recent trends in the development of new risk-related approaches, whether they are performed by the regulatory staff, nuclear industry, or other domestic or international bodies, are towards heavier emphasis in use of quantitative PRA results (interchangeably referred to as "risk measures" in this paper). It is well-known that quantitative results of PRAs, in particular, are subject to various types of uncertainties. Examples of these uncertainties include probabilistic quantification of single and common-cause hardware or software failures, occurrence of certain physical phenomena, human errors of omission and commission,

E-mail address: kamiar.jamali@hq.doe.gov

0951-8320/$ - see front matter Published by Elsevier Ltd.
doi:10.1016/j.ress.2010.04.001

magnitudes of source terms, radionuclide release and transport, atmospheric dispersion, biological effects of radiation, dose calculations, and many others. Unlike deterministic uncertainties related to physical phenomena (e.g., neutronics, thermal-hydraulics), PRA uncertainties are not readily reducible in most instances. Uncertainties associated with physical phenomena can often be reduced by tests, experiments, operating experience on actual or prototype designs, or improvements in analytical models or computational capabilities. Despite this well-known limitation, if quantitative PRA results are used in the context of risk acceptance criteria (i.e., when they are compared against a set of threshold values established by either the industry or the regulator), it would be difficult to counter the unambiguous but potentially misleading or incorrect message that is delivered by such a number-based process; i.e., implying that a design is unacceptable or unsafe because it did not meet a particular risk-based numerical threshold (labeled as a risk acceptance criterion).

An important issue that is outside of the scope of this paper, but is worthy of detailed discussions of its own, is that the introduction and impact of PRAs in the design and licensing stages for a future reactor is by and large different from the way that risk-informed regulations have been applied to existing reactors. Currently operating reactors had a deterministically established licensing basis (which included the plant's safety basis) before plant-specific or generic risk information and insights were made available through PRAs. The PRAs generally confirmed that the original deterministic approach to design and licensing was conservative (e.g., plants could respond to some accident scenarios in manners that were not credited in the deterministic analyses) and further identified changes that could improve plant design or operational safety. Meeting the deterministic requirements meant that implementation of their attendant provisions embodied within the concepts of defense in depth, safety margins, conservative assumptions and analyses, quality assurance, and numerous other factors (many of which are not readily measurable within a PRA model) created a safety cushion or margin that protected these plants from uncertainties, including those from "unknown unknowns" (for which a euphemism can be "emerging safety issues" as discussed in Section 2). On the other hand, PRA models have to rely on realistic inputs to ensure that risk significant insights are not obscured by artificially biased results derived from the application of uneven conservatisms. Therefore, great care must be exercised in bringing PRAs into the design process to ensure that the fundamental pillars of deterministic safety assurance process mentioned above are not unduly compromised. Thus, for future reactors, use of risk information can have a far more significant impact on the safety basis of the plant, including the potential to drive some key design decisions. The intent of risk-informed regulations is to ensure their influence is positive in safety tradeoff decisions.

2. NRC's approach to safety goals and risk acceptance criteria

NRC published the Safety Goals Policy Statement on August 8, 1986 [2]. While the text of this Policy Statement does use the phrase "acceptable risk," the title and the rest of the discussions were careful to avoid the use of the Quantitative Health Objectives (QHOs) of prompt fatalities (PFs) and latent cancer fatalities (LCFs) as regulatory risk-acceptance criteria. In other words, the selection of the terminology of "safety goals" was very deliberate. An important attribute of the calculation of plant-specific PFs and LCFs for comparison with the dual QHOs is that both are by necessity "integral" quantities that are derived from the contributions of all accident scenarios that are considered in the plant-specific PRA model.

The Commission's 1995 PRA Policy Statement on use of PRA methods in nuclear regulatory activities [3], which was issued in the aftermath of the completion of PRAs for all operating nuclear plants in accordance with the Individual Plant Examinations Generic Letter [4] states, in part:

> 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 complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
>
> The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

The Commission approved the staff's White Paper on Risk-Informed and Performance-Based Regulation in March 1999 [5], which provided definitions of risk-informed and risk-based regulations. It reiterates that the Commission does not endorse an approach that is risk-based, wherein decision-making is solely based on the numerical results of a risk assessment.

Regulatory Guide 1.174 [6] established the framework for risk-informed regulations in applications regarding making plant-specific changes to the licensing basis. Its approach ensures that numerical PRA results would not form the sole basis for making nuclear safety decisions by listing five key principles (i.e., meeting current regulations [which are primarily deterministic], meeting defense-in-depth principles, maintaining sufficient safety margin, keeping increases in risk small, and performance monitored) that have to be met for a risk-informed approach. Clearly, current regulations are by and large based on deterministic requirements. A key portion of the section on scope (Section 1.4) states:

> … The NRC has chosen a more restrictive policy that would permit only small increases in risk, and then only when it is reasonably assured, among other things, that sufficient defense in depth and sufficient margins are maintained. This policy is adopted because of uncertainties and to account for the fact that safety issues continue to emerge regarding design, construction, and operational matters notwithstanding the maturity of the nuclear power industry. These factors suggest that nuclear power reactors should operate routinely only at a prudent margin above adequate protection. The safety goal subsidiary objectives are used as an example of such a prudent margin.

The clause about continual emergence of safety issues for plants with many years of operating experience is an alternative way to state the concern regarding uncertainties about the "unknown unknowns" that are a more significant concern for future reactor designs.

One reason that Regulatory Guide 1.174 has worked well in application is that it was intended for operating plants with a primarily deterministic licensing basis already in place, which means that the plants were already determined to be safe before applying the results of plant-specific PRAs.

Finally, Note 2 of Chapter 19 of the Standard Review Plan (SRP) [7] states that the QHO-surrogates of Core Damage Frequency (CDF) and Large Release Frequency (LRF) are goals and not regulatory requirements.

The key conclusion from the above is that the NRC Commissioners have not endorsed a "risk-based" approach to regulation because of the uncertainties in quantitative results of