Progress in Nuclear Energy xxx (2017) 1–13

Contents lists available at ScienceDirect

Progress in Nuclear Energy

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

Impact of probabilistic risk assessment and severe accident research in reducing reactor risk

R.S. Denning [a, *], R.J. Budnitz [b]

[a] Consultant, 2041 Hythe Rd, Columbus, OH, USA
[b] Lawrence Berkeley National Laboratory, University of California, USA

ARTICLE INFO

Article history:
Received 6 March 2017
Received in revised form
11 May 2017
Accepted 23 May 2017
Available online xxx

Keywords:
Probabilistic risk assessment
Severe accident research
Societal risk
Risk reduction

ABSTRACT

The development of probabilistic risk assessment (PRA) as a safety analysis tool and the implementation of lessons learned from risk studies in the design, operation and regulation of nuclear power plants has resulted in a substantial reduction in reactor risk. The lack of a strong technical basis for realistically assessing severe accident behavior, including the release and transport of radionuclides to the environment, resulted in some conservatism in early risk studies that distorted the true nature of severe accident risk. This paper describes the evolution of PRA over the past four decades, the benefits that have been achieved in the reduction of reactor risk, and the changes in the perspective of the nature of severe accident risk associated with the development of a strong technical basis for assessing severe accident consequences. Based on these developments, we conclude that the probability of early containment failure leading to a large, early release of radioactive material to the environment was over stated in these early risk studies. Although it is not possible to preclude the possibility of offsite early fatalities in a severe accident, the probability is extremely small, perhaps below the level at which it should be a key consideration in regulatory oversight. Conversely, as highlighted by the Fukushima accident, the potential for the societal impacts of land contamination represents an important element of reactor accident risk that has received insufficient consideration in the past. These findings have implications regarding preferred strategies for emergency planning and appropriate metrics for risk-informed regulation.

1. Introduction

In many respects, the nuclear industry grew up too quickly. Initial operation of the Shippingport nuclear plant was followed quickly by the Connecticut Yankee plant, the first true pressurized water reactor (PWR) demonstration plant, and the Dresden plant, the first boiling water reactor (BWR) demonstration plant. Before these 300 MWe demonstration nuclear power plants (NPP) had begun to operate, 600 MWe plants and 800 MWe plants had already been ordered, soon to be followed by plants greater than 1000 MWe. As a result, it was not possible to incorporate significant operating experience into the design basis of subsequent generations of reactor designs. Thus, materials problems, such as steam generator tube degradation, and safety lessons, such as those exposed by the Browns Ferry Unit 3 fire and the Three Mile Island Unit 2 accident, had to be addressed by making expensive backfits to existing plant systems.

The objective of this paper is to assess the impact of two specific developments that have had a major impact on the safe design and operation of existing plants and have laid the groundwork for the improved safety of future plant designs: (1) probabilistic risk assessment (PRA) and (2) severe accident research. These developments have led to both a better understanding of the nature of severe accident risk and to an actual reduction in that risk. This paper only addresses the evolution in safety of light water reactors (LWRs), although an improved understanding of severe accident behavior and the application of risk analysis are playing a key role in the safe design of other advanced reactor concepts.

The nature of the hazard associated with the large inventory of radioactive material in an operating nuclear power plant is significantly different from the safety challenge posed by other forms of electricity generation. This difference was recognized by the designers very early through the development of a Defense-in-Depth (Drouin et al., 2016) approach to assuring adequate public safety (as

* Corresponding author.
E-mail address: denningrs.8@gmail.com (R.S. Denning).

http://dx.doi.org/10.1016/j.pnucene.2017.05.021
0149-1970/

described in Section 2). However, the plants that are currently operating were largely designed, constructed and operated without an in-depth capability to model the response of the plant to off-normal, low probability events beyond the design basis of the plant.

1.1. Risk

Risk is defined as "the possibility that something bad will happen," (Merriam-Webster Dictionary, 2017). *Risk* always has two elements, a consequence characteristic and a likelihood characteristic. When someone assesses whether an action is "safe" or "unsafe", they are actually assessing what the risk of the action is. Thus, when we describe an improvement in reactor safety, we are implying an improvement in reactor risk, either a reduction in probability, a reduction in consequences or a reduction in both. When we cross a street, there is a potential consequence that we will be struck by a car and die (perhaps the ultimate consequence), but by taking appropriate precautions (staying in the cross walk; looking both ways) we determine that the probability of being struck is sufficiently low that we conclude it is safe to cross. We briefly address "safety adequacy" in this paper within the context of the conformance of plant risk to probabilistic safety goals that have been established by the Nuclear Regulatory Commission (NRC). Nevertheless, the question of safety adequacy underlies basic decisions made by owners, regulators and the public in deciding whether or not to maintain or expand the role of nuclear energy in addressing future energy supply needs.

As the result of extensive severe accident research, reactor operating experience, and the application of risk assessment techniques, our technical understanding of reactor accident risk has substantially improved over the past sixty years. The primary value of a risk assessment is generally recognized as the identification of the principal contributors to risk rather than the quantitative (bottom line) results. In fact, risk analysts generally warn against over-emphasis on the calculated risk numbers without consideration of the associated uncertainties. Nevertheless, in this paper we will use the quantitative results from risk assessments to provide a measure of the relative improvement (reduction) in risk that has occurred as a result of changes in plant configuration and plant operations.

The second major topic discussed in this paper is the insight, which has evolved through an extensive body of both experimental and analytical studies, that the likelihood of a major accident that would produce a very early and large release of radioactive material to the environment is much less than had been thought earlier. Conversely, another insight is that the importance of major contamination to off-site property has not received the degree of attention it deserves, either in the regulations or in the considerations of decision-makers at the policy level. The bases for these insights will be discussed in the body of this paper.

The fact that there is an improved technical understanding of NPP risk does not necessarily mean that public *perception* of the risk of NPP accidents has changed. Communicating a technical understanding of risk to the public is extremely difficult. Thus, we will differentiate between a technical understanding of the magnitude of risk, which is the subject of this paper, and public perception of risk.

1.2. Structure of paper

Section 2 of this paper describes the deterministic framework that was developed for the regulation, design and operation of NPPs. Section 3 describes the methodology of PRA, including a description of WASH-1400, the first major application of PRA to address the risk of commercial NPPs (US NRC, 1975). Because of the very limited knowledge of severe accident behavior that existed at the time WASH-1400 was undertaken, before PRA could become a reliable tool for safety regulation it was necessary to undertake sufficient research on severe accident behavior to assure that PRA was not leading to a distorted perspective of the contributors to plant risk. The scope of this research is described in Section 4. Section 5 returns to a discussion of PRA and its broad application to NPPs in the U.S. Section 6 provides our quantitative assessment of the actual reduction in risk of accidents in NPPs currently operating in the U.S. that has resulted from actions taken based on PRA results. This improvement in the understanding of reactor risk has also provided the basis for a future generation of LWRs with even lower risk. Finally, in Section 7 we discuss general misperceptions of the nature of the risk posed by operating plants and provide our own perspective.

2. Development of a regulatory framework, deterministic design criteria, and operating restrictions for U.S. reactors

The regulatory requirements imposed by the U.S. Nuclear Regulatory Commission (NRC) on the safe design, licensing and operation of nuclear power plants are contained in Title 10, Part 50 of the Code of Federal Regulations (US NRC, 2017a). Appendix A to Part 50 identifies General Design Criteria (GDC) that are applicable to all NPPs in the U.S. The GDC codify a safety philosophy built around the use of multiple barriers to the release of radioactive material, a balance of preventive and mitigative safety features, and the use of redundancy and diversity of safety systems. Although the term Defense-in-Depth was not coined until the late 1960s, it is now used as a general description of this underlying approach to NPP safety (Drouin et al., 2016). Some of the key requirements of the GDC are a high level of quality assurance (as detailed in Appendix B of Part 50), protection against natural phenomena hazards, fire protection, leak-tight containment system, emergency core cooling system, negative reactivity feedback, independent reactor shutdown system, and decay heat removal system.

In complying with the GDC and more detailed regulatory guidance documents, *deterministic* design bases are developed by the reactor design organization for safety-related systems. For example, based on a calculation of the increase in pressure that would occur in containment in a major loss of coolant accident of 0.25 MPa, a design basis for the containment might be 0.3 MPa, which includes some safety margin based on established safety codes developed by industry organizations, like the American Concrete Institute. These codes and standards have undergone extensive review by standards committees. The design bases for a nuclear power plant are described in a Safety Analysis Report (SAR) in which compliance with the design bases is demonstrated by the analysis of so-called "design basis accidents." The SAR also includes Technical Specifications that describe the Limiting Conditions of Operation of the plant, such as an identification of the number of safety trains that must be in service for the plant to continue to operate at full power. One of the key design requirements for an NPP is assurance that safety functions can be satisfied even if any single component has failed. This requirement is referred to as the Single Failure Criterion. It is an essential element of the NRC's deterministic approach to safety, in order to provide protection under circumstances in which it is necessary to disable a train of a safety system to perform testing or maintenance while the plant is operating. It also provides protection against a condition in which a safety-related component has failed but its failure has not yet been identified. The Single Failure Criterion is only applied to "active" components, i.e. those components that require some motive force like electricity or a steam turbine or require operator intervention to operate.

Please cite this article in press as: Denning, R.S., Budnitz, R.J., Impact of probabilistic risk assessment and severe accident research in reducing reactor risk, Progress in Nuclear Energy (2017), http://dx.doi.org/10.1016/j.pnucene.2017.05.021