Annals of Nuclear Energy 110 (2017) 979–988

Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

Whether a Theory of Nuclear Safety is deterministic or probabilistic? A metatheory

Gangyang Zheng [a,b,*], Paul Nelson [b], Ernie Kee [b,c], Fatma Yilmaz [c], Zhijian Zhang [a], Martin Wortman [b]

[a] Harbin Engineering University, Harbin, Heilongjiang 150001, China
[b] Texas A&M University, College Station, TX 77840, USA
[c] South Texas Project Nuclear Operating Company, Wadsworth, TX 77480, USA

ARTICLE INFO

Article history:
Received 6 April 2017
Received in revised form 7 August 2017
Accepted 9 August 2017
Available online 17 August 2017

Keywords:
Nuclear safety
RISMC
Theories of nuclear safety
Safety margin

ABSTRACT

Theoretical criteria for design or regulatory safety of nuclear power plants often take the form of requirements that some model of the "capacity" of the plant to respond to a hypothesized threat sufficiently exceed a model of the "load" presumably placed upon the plant by that threat. Either of capacity or load can be deterministic or probabilistic, which leads to a four-type typology, as opposed to the traditional classification of theories of nuclear safety as either deterministic or probabilistic. Concrete examples of each of the four types are provided. Possible uses of this viewpoint for design and regulation are discussed, especially as regards melding of the basically deterministic notion of safety margins with its natural probabilistic counterpart of requiring load exceed capacity with only very small probability. Use of this viewpoint is illustrated by using it as a framework within which to describe the regulatory impact of the well-known ECCS hearings of the 1970s.

1. Introduction

By a "Theory of Nuclear Safety" (TONS), this work intends very broadly any set of principles for the systematic design or regulation of nuclear power plants (NPPs) so as to achieve adequately safe operation. The motivation for introducing a theory of theories of nuclear safety (TONSs - other plural acronyms will be used similarly), which is to say a metatheory of nuclear safety, is to permit a focus upon questions that cut across all TONSs. Specific instances of such questions of interest here are how safety should be measured, or the relationship between different approaches to measuring safety. Such measurement issues obviously are fundamental to familiar endeavors such as risk assessment (how much safety is achieved) or risk management (how much safety is needed).

The specific objectives of the present work are:

1. to suggest a typology of TONSs that generalizes the traditional classification of safety or risk analyses into deterministic or probabilistic (e.g., Hess et al. (2009a)), as suggested by the basic concepts of Risk-Informed Safety Margin Characterization (RISMC) (Hess et al., 2009a, 2011; Smith, 1998) (cf. Section 2) and to note examples of each of the (four) types that represent current practice (Section 3 below);
2. to describe (Section 4) and illustrate (Section 5) how this typology can be used to frame discussion of issues related to nuclear safety, especially as regards relationships between two well-known measures of nuclear safety, safety margins (for deterministic analyses) and probability of failure (for probabilistic analyses).

The internationally accepted consequence-focused traditional classification of risk assessments into Levels 1, 2 and 3 also merits note (Solanki and Prasad, 2007), although it will not play a role here. In the following Section 2 the rudiments of RISMC, as foundational to the typology of Section, are collected, along with references to relevant earlier work.

2. Context and related work

A fundamental precept of RISMC (e.g., Hess et al. (2009b)) is that the criterion for system failure, in responding to a particular type of Initiating Event (IE), can be formulated as that some "load" (or "demand") imposed by the IE upon the various backup safety systems intended to respond to such IEs exceed some commensurately measured collective "capacity" of those backup systems to

* Corresponding author at: Harbin Engineering University, Harbin, Heilongjiang 150001, China.
E-mail address: reliabilityzheng@foxmail.com (G. Zheng).

http://dx.doi.org/10.1016/j.anucene.2017.08.014
0306-4549/

Nomenclature

CCF	Common-Cause Failure
CDF	Core Damage Frequency
cdf	cumulative distribution function
CFR	Code of Federal Regulations
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
DBA	Design Basis Accident
GSI	Generic Safety Issues
IE	Initiating Event
LERF	Large Early Release Frequency
LOCA	Loss of Cooling accident
LOOP	Loss of Offsite Power
MCL	Maximum Credible Load
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
P_f	Probability of failure
Pr	probability
P_s	Probability of success
PSA	Probabilistic Safety Analysis
PSP	Pressure Suppression Pool
RISMC	Risk-Informed Safety Margin Characterization
rcry	reactor critical year
SBO	Station Black Out
TONS	Theory of Nuclear Safety

respond to the circumstance created by the IE. The failure criterion is that some component of load exceeds the corresponding component of capacity.

The RISMC methodology that prescribes about utilization of the capacity and load concepts risk assessment is conceptually identical to the stress-strength interference concept that has been utilized in many fields of engineering, perhaps particularly structural engineering (Haldar and Mahadeven, 2000). In the latter field it often is termed as *risk-based design* (Riesch-Oppermann and Brückner-Foit, 1988; Brückner-Foit et al., 1989). Some emphasis on this view within nuclear energy has recently emerged through the RISMC pathway (Idaho National Laboratory, 2012) under the U.S. DOE Light-Water Reactor Safety program. Additionally, the literature (Pagani, 2004) shows instances of the methodology of risk-based design being employed to address isolated but specific technical issues.

Most fundamentally, capacities and loads are random variables whose distributions are known, to some approximation, through a combination of operational data, controlled experimentation, and, perhaps some theory, often in the form of computational modelling. Capacities and loads can be, and often are, modelled as having deterministic ("point") values, especially for loads or capacities primarily determined by computational modeling. Especially, some of the computational burdens associated to using distributed loads for calculations of probabilities (or frequencies) of system failure often have been bypassed by employing "maximum credible" deterministic ("point") values of load that are considered to provide *de facto* conservative upper bounds to those probabilities or frequencies. For these reasons it is customary and arguably important in nuclear safety to distinguish between deterministic and probabilistic models of load and capacity.

The suggestion here is that such models also can be considered as instances of a finer subdivision of TONS comprising mixed types, in which one of load or capacity is deterministic, while the other is probabilistic, as well as the purely deterministic or purely probabilistic types. Mixed types are theoretically possible, and in fact often employed, albeit usually tacitly.[1]

Risk assessment techniques were already being used to some extent in the NRC's regulatory process (Levine, 1979). On their webpage (U.S. Nuclear Regulatory Commission, 2016), the U.S. Nuclear Regulatory Commission (NRC) states their intent toward transitioning to risk-informed regulation as follows: "Many of the present regulations are based on deterministic and prescriptive requirements that cannot be quickly replaced. Therefore, the current requirements are being maintained, while risk-informed and/or performance-based regulations are being developed and implemented. In the following (i.e., on the NRC webpage), examples are shown where the probabilistic and deterministic approaches are mixed or fully implemented (fully probabilistic or fully deterministic)." Furthermore, in Section 4, it is documented that knowledgeable individuals perceive this transition as occurring at a somewhat deliberate pace, and some possible theoretical basis for this being due to a natural tension between the deterministic and probabilistic approaches to regulation for safety is developed.

Sherry et al. (2013) provides and describes a perspective from which an NPP owner-operator might naturally be led to consider a TONS in which capacity is deterministic, while load is probabilistic, while a regulator might equally well consider the exact same IE from the perspective of a probabilistic-capacity deterministic-load TONS. The connecting link between the two is provided by the notion of some (presumably mutually agreed) "safety limit". From the perspective of a NPP owner-operator this safety limit can be taken as a deterministic capacity that is fixed, while the probabilistic load is a random variable whose distribution can be adjusted (e.g., by power uprating) "to achieve enhanced plant operational and economic performance," so long as the probability that the load exceeds the safety limit remains negligibly small. Similarly, the regulator can view the safety limit as a deterministic load, with the capacity as a random variable whose distribution can be adjusted by the regulator, so long as the probability that the capacity falls below the safety limit remains sufficiently small. (See Nuclear Energy Agency (2007), Ma et al. (2009) for illustrative applications of this idea; the sample application described in Ma et al. (2009) actually is a probabilistic-capacity probabilistic-load TONS, with a relatively simple distribution for the capacity but a complex distribution for the load that is determined empirically by applying sophisticated sampling techniques to a state-of-the-art system analysis computer code.)

3. Instances of the four types

In the first of the following subsections it is argued that the instance of a TONS comprised of the traditional deterministic approach to assessment of the adequacy of the Emergency Core Cooling System (ECCS) of a NPP to respond to a Loss of Coolant Accident (LOCA) event can be viewed as a deterministic-capacity

[1] By contrast, we would not consider a purely prescriptive approach to regulation to be an instance of a TONS. That is not intended to downplay the utility and importance of prescriptive approaches, but rather because we consider a TONS to be fundamentally quantitative, whereas a prescriptive approach is intrinsically qualitative. In the regulatory context the terms "prescriptive" and "deterministic" often are not clearly distinguished, and sometime even treated as identical, which is a practice we consider ill-suited to clarity of thought and expression.