Annals of Nuclear Energy xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

The study of meta-theory of nuclear safety in one single Initial Event

Gangyang Zheng, Zhijian Zhang *, Chengming Hao, Xiaomeng Dong, Huazhi Zhang, Yingfei Ma

Harbin Engineering University, China

ARTICLE INFO

Article history:
Received 22 June 2016
Received in revised form 7 December 2016
Accepted 15 March 2017
Available online xxxx

Keywords:
Nuclear safety
Theory of nuclear safety
RISMC
LOCA
Initial Event

ABSTRACT

The purpose of this paper is to extend the meta-theory of theory of nuclear safety to a new stage. Meta-theory method describes nuclear power plant's nuclear safety systematically and is devised to analyze and to assist the investigation of the theory of nuclear safety. Different types of "capacity" and "load" via RISMC method were present by meta-theory, which could be found out from the real examples that one of load and capacity is deterministic, while the other is probabilistic. In the current research, the authors intend to develop all four combinations in one single Initial Event, aiming to extend this meta-theory method to a more extensive and practical level. A methodology has been verified by a specific yet simple engineering case, i.e., LOCA. To validate its logic, we present an Event Tree to explain the different responses of different safety systems. Then, RELAP 5 is programmed to establish a traditional LOCA sequence to investigate the changing situations of various parameters in reactor coolant system. Based on these approaches, the "capacity" and "load" should be described and all the four "capacity – load" cases in an Initial Event are determined.

1. Introduction

The rudiments of meta-theory of theory of nuclear safety (TONS) are contained in two taxonomies which are Deterministic Safety Analysis (DSA) or Probabilistic Safety Analysis (PSA). This research intends to develop this systematic methodology to analyze the safety of Nuclear Power Plant (NPP), or to assist the investigation of TONS. The safety analyses are classified as either "deterministic" or "probabilistic" (e.g., Hess et al. (2009a)), and the latter designations seem to be accepted widely (Solanki and Prasad, 2007). Furthermore, this theory is also based on Risk-Informed Safety Margin Characterization (RISMC). According to the attributes of capacity and load, which are the fundamentals of RISMC, these two types of TONS are considered as quite distinct.

Some hybrid methods combining probabilistic and deterministic methods have already been applied in NPP's reliability, economic analysis and safety design field. However, the model uncertainty and the accompanying over-conservatism will always make the cost of nuclear facilities undesirably higher. Therefore, the industry needs to reevaluate its level to obtain an optimized design via a probabilistic design and an optimization approach (Reinert and Apostolakis, 2006). It has also been investigated through the Risk-Informed probabilistic design approach for several kinds of safety systems of NPPs (Martorell and et al., 2002). Meanwhile, deterministic design philosophy is adopted to address safety concerns and is accepted by all stakeholders.

The present work outlines a meta-theory framework that extends the traditional DSA/PSA categories in a manner broadly based upon what we take as the basic precept of RISMC (Hess et al., 2009a,b). Then, the current paper mainly develops a systematic methodology for analyzing the safety of a NPP, especially in one single Initial Event. In a specific Initiating Event, the accident sequence could be determined by the classical PSA analysis and the design assessment in DSA scope. That rule here is taken as the appropriate metric for the degree of safety provided by an Engineered Safety Facility (ESF) (or safety system/subsystem). For analyzing and demonstrating the effectiveness of meta-theory, we focus on the ESFs and consider the response first. When all kinds of systems or subsystems respond to the failure modes which are caused by Initiating Event, it is necessary to describe the produced "capacity" and "load" according to the related operations (normal operation), as well as the relationship between them, and determine the appropriate numerical "capacity" and "load". Some measures of the amount by which the capacity of that subsystem to respond to failure of some safety-related normally operating subsystem exceeds the load imposed by that failure. All the variation of physical parameters and the response of all kinds of ESFs are presented in a RELAP 5 Mod 3.4 model, which is used to establish a traditional LOCA sequence in reactor coolant system. In this framework, after presenting a simple Event Tree

* Corresponding author at: Harbin Engineering University, College of Nuclear Science and Techonology, 150001, China.

E-mail address: zhangzhijian_heu@hrbeu.edu.cn (Z. Zhang).

http://dx.doi.org/10.1016/j.anucene.2017.03.026
0306-4549/

Please cite this article in press as: Zheng, G., et al. The study of meta-theory of nuclear safety in one single Initial Event. Ann. Nucl. Energy (2017), http://dx.doi.org/10.1016/j.anucene.2017.03.026

Nomenclature

CDF	core damage frequency
DSA	deterministic safety assessment
ESF	engineered safety facility
ET	event tree
LOCA	loss of coolant accident
NPP	nuclear power plant
PSA	probabilistic safety analysis
RISMC	risk-informed safety margin characterization
TONS	theory (or theories) of nuclear safety

(ET) analysis to explain the different response situations of different safety systems (or ESFs), four types of "capacity – load" could be found based on the fundamentals of meta-theory of TONS, which include: i) (Probabilistic-capacity Deterministic-load) case; ii) (Deterministic-capacity Deterministic-load) case; iii) (Probabilistic-capacity Probabilistic-load) case; and iv) Deterministic-capacity Probabilistic-load) case; i.e., (P, D), (D, D) (P, P) and (D, P) in one single Initiating Event. The reason comes from "Level 1 PSA models determine Core Damage Frequency (CDF) based on Initiating Event analysis, scenario development, system analyses, and human-factor evaluations (From p. 4 of Nuclear Electric Institute (2005))."

This paper is organized as follows. The description of meta-theory which contains four types of cases is presented in Section 2. Then, Section 3 ("Classical Large LOCA") presents a simple ET to explain the different response of different ESF (or safety subsystem) to state the selected Initiating Event. Its failure sequence and the response of the ESFs are also discussed in Section 3. After that, through the RELAP 5 model, the accompanying Section 4 contains examples of commonly employed TONS of all four types in one single Initiating Event. In Section 5 ("Measures of Safety"), their mathematics and physics implications which contains a discussion of generalizations of measures of nuclear safety are deduced by the specially Initiating Event case. The last Section is Concluding Remark.

2. Mixed types in nuclear safety theory

Nuclear safety is ensured through deterministic safety principles of Defense in Depth and the Single Failure Criteria (Nuclear Regulatory Commission, 2015). However, in the real engineering practices, such as construction and operation, new challenges prove to affect the dependability of the original safe design. With the development of Risk-Informed technique, the hybrid taxonomies method has evolved by itself (Stephen Hess et al., 2011). For instance, safety limit can be taken as a deterministic capacity which is fixed, while the probabilistic load is a random variable whose distribution can be adjusted from the perspective of a NPP owner-operator (e.g., by power uprating) "to achieve enhanced plant operational and economic performance" (Sherry et al., 2013), 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 (Nuclear Regulatory Commission, 2002), as long as the probability that the capacity falls below the safety limit remains sufficiently small.

The suggestion here is that they should be considered as instances of a broader class of TONS comprising both the mixed types, and the purely deterministic or purely probabilistic types. Clearly such mixed types are theoretically possible; and has practical values as well.

The previous work (also led by the authors) had already outlined this meta-theory framework (Zheng et al., 2013), but we found that all the four types "capacity – load" cases in one single Initiating Event are different from the various Initiating Events in the previous work as mentioned. The basic event would emerge, and at this point, Risk-Informed method and RISMC, which are regarded as a composited method has been gradually concerned. In addition, the analytical studies are the PSA and Risk-based studies which establish the dependability of the designs of NPPs.

For any particular safety subsystem, it is necessary to identify appropriate quantities corresponding to capacity and load. The primary objective of this work is to observe that both capacity and load can be a deterministic or a probabilistic variable independently. Meanwhile, real examples of analyses are used in nuclear industry which all four of the corresponding combinations actually occur. And then, the process begins with the selection of a set of Initiating Events which have the potential to start an accident scenario. For example, the internal Initiating Event of "Loss of Coolant Accidents (LOCA)" generally refers to events involving breaks of coolant channels of various sizes. This leads to the loss of primary heat transport water from the coolant channels, which subsequently causes a reactor trip. Hence, a secondary objective of this paper is to discuss the possibility of the four types in one single Initiating Event and to pursue the logic of "probabilistic" and "deterministic".

3. Classical large LOCA

In this section, we select the large break LOCA as an example. Large break LOCA is a very important accident in nuclear safety area. Its analysis has been very mature among the entire international nuclear engineering field, and its accident sequence and time processes were widely studied (Srinivas et al., 2011; Gonzalez-Cadelo et al., 2014). Therefore, it is selected as a start point to set a single event in the study. In this Initiating Event, all kinds of "capacity" and "load" which are caused by the responses of ESFs or specific safety (sub) systems, would be analyzed gradually, along with the progression of the accident sequences.

In the process of identifying accident scenarios, the possible responses of the NPP to the occurrence of an Initiating Event are modeled by employing the ETs. Each branch point of the ET represents the possibility that the corresponding frontline system (or function) may or may not be available. For the failure branches (by convention the downward branch is taken as the failure branch), the failure modes of the frontline systems are defined and Fault Tree analysis is employed to find possible combinations of component failures and/or human errors that might lead to these failures. In this research, large break LOCA is chosen as a specified Initiating Event to launch the accident analysis (Srinivas et al., 2011). In general, when it is selected, the accident sequence would be determined.

The paths in the ET define the accident sequences. Each of these sequences leads to a "plant state", i.e., a particular state of the nuclear reactor that defines a set of initiating and boundary conditions for later analysis. Thus, when the large break event occurs, first of all, the primary operation step is to shut down the reactor,