Annals of Nuclear Energy 122 (2018) 175–184

Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

Development of a quantitative resilience model for nuclear power plants

Ji Tae Kim [a], Jooyoung Park [b], Jonghyun Kim [b], Poong Hyun Seong [a,*]

[a] Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science Technology, 291 Daehak-ro, Yuseong-gu, Deajeon 34141, Republic of Korea
[b] Department of Nuclear Engineering, Chosun University, 309 Pilmun-daero, Dong-gu, Gwangju 501-709, Republic of Korea

A R T I C L E I N F O

Article history:
Received 1 May 2018
Received in revised form 6 August 2018
Accepted 22 August 2018

Keywords:
Resilience
Safety-I
Safety-II
Nuclear power plant

A B S T R A C T

The causes of the Fukushima nuclear power plant (NPP) accident have been identified as not only technical factors such as the structure, system, and equipment design, but also inadequate management of the human and organizational factors, which were the major contributors to exacerbating the beyond design basis accident. After the accident, the safety paradigm was changed to address the failure of equipment as well as effective factors for safety. Resilience engineering is a relatively new paradigm for safety management that focuses on how to cope with complexity under pressure or disturbance to achieve success, addressing the limitations of existing safety analysis measures. This study aimed to develop a quantitative resilience model for the NPP using a modified NPP resilience model based on the Model of Resilience in Situation developed by the Électricité de France. Event reports for Korea NPPs were analyzed according to the perspectives of Safety-I and Safety-II, and statistical analysis was performed to identify the relations in the resilience model. Through this analysis, the quantitative relationship of the element in the resilience model was determined, and the quantitative resilience model was developed. The developed quantitative resilience model was also validated through a statistical method. Our results provide a new method for safety assessment in NPPs, which can complement the conventional safety assessment. The proposed method is expected to be an index for evaluating the integrity of safety management in Korean NPPs.

1. Introduction

A nuclear power plant (NPP) is a safety–critical organization whose main objective is to control hazards and risks that can cause the release of radioactive elements into the environment. The causes of the Fukushima NPP accident have been identified as not only technical factors such as the structure, system, and equipment design but also insufficient management of the human and organizational factors, which were the major contributors to exacerbating the beyond design basis accident. After the Fukushima NPP accident, three recommendations were suggested as a result of a meeting of international experts of the International Atomic Energy Agency (IAEA): 1) revision of the IAEA safety guidelines and standards for human and organizational factors, 2) development of organizational resilience guidelines reflecting the state-of-the-art research, and 3) development of a method for assessing the human and organizational factors for a stress test (IAEA, 2013). An IAEA report highlighted the necessity of a paradigm shift regarding safety in NPPs (IAEA, 2013). This report recommended a systemic approach to address the safety of the whole system by considering the dynamic interactions within and among all the relevant factors of the system, including individual factors (e.g., knowledge, thoughts, decisions, actions), technical factors (e.g., technology, tools, equipment), and organizational factors (e.g., management system, organizational structure, governance, resources). Thus, after the Fukushima NPP accident, the safety paradigm was changed to address the failure of equipment as well as effective factors for safety.

The definition of safety is the state of being safe, which is the condition of being protected from harm or other non-desirable outcomes. From the concept of Safety-I, increasing safety means reducing the number of failures by precautionary measures such as rigid policies, more rules, and additional constraints. However, safety management and evaluation may not be applicable for highly complicated systems such as NPPs. They may limit the ability of the people working in the highly complicated system to adapt, thereby unintentionally creating a more brittle and less flexible system (Wears, 2015). Erik Hollnagel, David Woods, and Nancy Leverson suggested that safety management should transition from ensuring that “as few things as possible go wrong” to ensuring that “as many things as possible go right” (Hollnagel et al., 2013). This perspective is defined as Safety-II and is related to

* Corresponding author.
E-mail addresses: jitae5@kaist.ac.kr (J.T. Kim), zxas1156@chosun.kr (J. Park), jonghyun.kim@chosun.ac.kr (J. Kim), phseong@kaist.ac.kr (P.H. Seong).

https://doi.org/10.1016/j.anucene.2018.08.042
0306-4549/

the ability of the system to mitigate varying situations. The concept of Safety-II assumes that the performance variability provides the adaptations that are needed to respond to various situations; therefore, it focuses on the condition that "things go right." Human factors are consequently considered as resources necessary for system flexibility and resilience (Hollnagel et al., 2015).

Resilience can be defined as the intrinsic ability of a system to adjust its operation prior to, during, or following changes and disturbances, so that it can sustain required operation under both expected and unexpected conditions (Hollnagel, 2011). Resilience engineering is a relatively new paradigm for safety management that focuses on how to cope with complexity under pressure or disturbance to achieve success (Hollnagel, 2009). There are several limitations of existing safety analysis measures, such as deterministic safety analysis (DSA) and probabilistic safety assessment (PSA). For instance, the existing safety analysis measures focus on the failure of the system and try to eliminate the causes of failure. They also consider the failure of components and human error and assess these factors individually. In contrast, resilience engineering focuses on the success of the system and aims to eliminate the latent factors that can be trigger a disaster. It involves an overall assessment, considering the hardware, operator, organizational, training, procedure, etc. Additionally, it assesses the integrated safety-influencing factors. Thus, resilience engineering provides a more integrated view for safety analysis. It focuses on what the organization does well, i.e., what it does to maintain its successful operation, and exploits these processes in the event of an unexpected situation.

The objective of this study is to develop a quantitative resilience model. In the course of the study, data analysis on the factors of a resilience model from the Safety-I and Safety-II perspectives was performed. The quantitative resilience model was derived from the analysis result according a statistical method. The statistical method was also used to validate the proposed quantitative resilience model.

2. Structure of resilience model

The authors' previous work suggested and characterized a resilience model that was modified from a resilience model of Électricité de France (EDF) (Park et al., 2018). It also performed a correlation analysis for the model and showed a feasibility of the concept of Safety-II. This study is a follow-up of the previous work. This section briefly introduces the structure of the resilience model.

2.1. Resilience model of EDF

EDF developed a resilience model that considers emergency operating systems (EOSs) and their interactions with NPPs. The resilience model is a "Model of Resilience in Situation" (MRS) that categories human behavior and the relevant factors influencing the EOS resilience during an emergency situation (Le Bot, 2007). It describes the management of a high-risk situation based on an ongoing process described by functions that are ensured by the control system and the organization via its management, before and after the occurrence of these situations. The MRS shown in Fig. 1 consists of five resilience attributes: anticipation, adaptation, collective functioning, robustness, and learning organization.

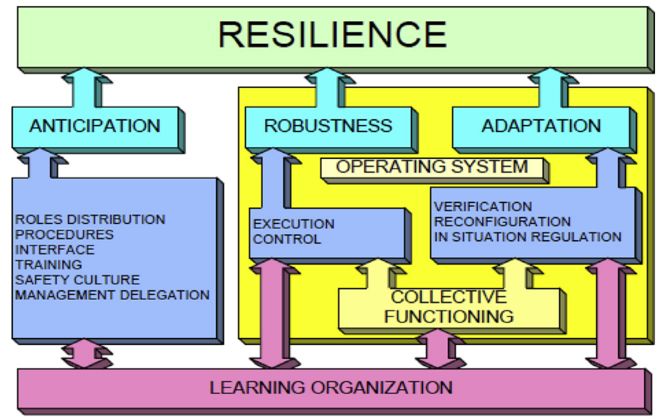

Fig. 1. MRS developed by EDF.

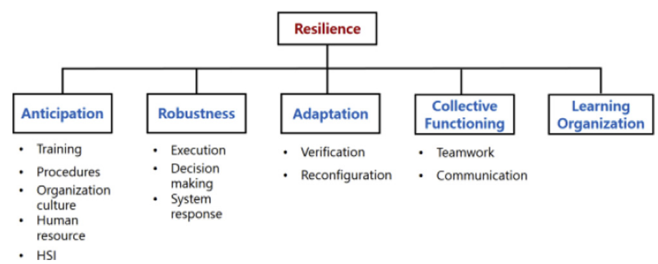

Fig. 2. Structure of a resilience model for an unexpected situation in NPPs.

2.2. Resilience model used in this study

The resilience model for unexpected situation in NPPs considered in this study is modified from the MRS of EDF (Kim et al., 2009, Kim et al., 2017). As shown in Fig. 2, this model consists of five high-level attributes and corresponding low-level factors with three levels. Resilience is placed at the top. The second level contains five attributes: anticipation, robustness, adaptation, collective functioning, and organizational learning, which are characterized by their properties. At the third level, the elements of each attribute are defined. Their characteristics and explanations for the factors and attributes are as follows.

2.2.1. Anticipation

Anticipation characterizes the measures that are in place before an initiating event occurs and is therefore a measure of the preparedness of the EOS before an event. Competent personnel, sufficient hardware, and good organization are required to identify issues that can become threats and then prevent the threat from occurring. Anticipation includes the NPP operation procedures, the training program of the operators, and human resources, as it impacts the crew behavior in response to an initiating event. It consists of training, procedures, organization culture, human resources, and human–system interfaces (HSIs).

Training refers to the knowledge and experience imparted to the personnel by the organization. Training content, scheduling, and frequency should be considered when establishing a training program. Operator training is crucial for ensuring the safe and reliable operation of NPPs.

Procedures provide descriptions of the tasks that should be performed and the rules that should be followed to address specific conditions in NPPs. They provide instructions to guide operators in decision-making and monitoring and controlling the plant and can reduce human errors.

Organizational culture comprises the attitudes, values, and beliefs of an organization that support its goals and mission. Because plant safety is the primary goal of emergency operations, the safety culture of the organization is highlighted in its EOS.

Human resources refer to the way that the organization hires and assigns tasks to personnel (Reason, 1997). Staffing issues