Nuclear Engineering and Design 315 (2017) 20–34

Contents lists available at ScienceDirect

Nuclear Engineering and Design

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

Probabilistic risk assessment framework for structural systems under multiple hazards using Bayesian statistics

Shinyoung Kwag [a,b], Abhinav Gupta [a,*]

[a] North Carolina State University, Raleigh, NC 27695, USA
[b] Korea Atomic Energy Research Institute, Daejeon 305-353, Republic of Korea

HIGHLIGHTS

- This study presents the development of Bayesian framework for probabilistic risk assessment (PRA) of structural systems under multiple hazards.
- The concepts of Bayesian network and Bayesian inference are combined by mapping the traditionally used fault trees into a Bayesian network.
- The proposed mapping allows for consideration of dependencies as well as correlations between events.
- Incorporation of Bayesian inference permits a novel way for exploration of a scenario that is likely to result in a system level "vulnerability."

ARTICLE INFO

Article history:
Received 10 October 2016
Received in revised form 31 January 2017
Accepted 4 February 2017

Keywords:
Multi-hazard risk assessment
Bayesian networks
Bayesian inference
Vulnerability beyond design basis

ABSTRACT

Conventional probabilistic risk assessment (PRA) methodologies (USNRC, 1983; IAEA, 1992; EPRI, 1994; Ellingwood, 2001) conduct risk assessment for different external hazards by considering each hazard separately and independent of each other. The risk metric for a specific hazard is evaluated by a convolution of the fragility and the hazard curves. The fragility curve for basic event is obtained by using empirical, experimental, and/or numerical simulation data for a particular hazard. Treating each hazard as an independently can be inappropriate in some cases as certain hazards are statistically correlated or dependent. Examples of such correlated events include but are not limited to flooding induced fire, seismically induced internal or external flooding, or even seismically induced fire. In the current practice, system level risk and consequence sequences are typically calculated using logic trees to express the causative relationship between events. In this paper, we present the results from a study on multi-hazard risk assessment that is conducted using a Bayesian network (BN) with Bayesian inference. The framework can consider statistical dependencies among risks from multiple hazards, allows updating by considering the newly available data/information at any level, and provide a novel way to explore alternative failure scenarios that may exist due to vulnerabilities.

1. Introduction

In a probabilistic safety assessment (PSA) or probabilistic risk assessment (PRA) (USNRC, 1983; IAEA, 1992; EPRI, 1994; ASME/ANS, 2009; ASCE, 2016; Fullwood, 2000; Ellingwood, 2001), the risk metric for a specific hazard can be evaluated by convolution of system fragility and hazard curves. The hazard curve expresses the annual probability of exceedance as a function of the intensity measure employed to characterize the hazard. The fragility curve of an event is expressed in terms of the conditional probability of failure as a function of the intensity measure for a given hazard and is obtained by considering uncertainties in the available physical model of a component or system through the use of empirical, experimental, and/or numerical data. US Nuclear Regulatory Commission and International Atomic Energy Agency have issued guidelines for conducting a full scope PRA (EPRI, 1994; IAEA, 1992). In this methodology, the plant level risk is calculated by a combining the component and subsystem fragility curves through a systems analysis. Typically, fault and event trees are used for conducting the systems analysis to combine the fragilities and convoluting with the hazard curve.

The currently used methodology is focused on addressing the risk associated with each external hazard separately. Multi-hazard scenarios have not been considered in a traditional PRA study because the possibility of simultaneous occurrence of two different extreme events such as earthquake and hurricane or earthquake and floods is extremely rare and almost impossible.

* Corresponding author.
E-mail address: agupta1@ncsu.edu (A. Gupta).

http://dx.doi.org/10.1016/j.nucengdes.2017.02.009
0029-5493/

However, there have been several instances of closely-related multiple hazards that have resulted in significant damage or a major disaster. Seismically induced flooding due to tsunami following the great Tohoku earthquake caused the disaster at Fukushima Daiichi nuclear plant (Aoki and Rothwell, 2013). One may argue that such a multi hazard scenario though very recent is also quite rare and limited to very specific regions in the world. On the other hand, there are many instances of significant damage or a major disaster due to seismically induced internal flooding such as those due to failure of fire piping or tanks in a hospital or other industrial facilities. Seismically induced fires are widely acknowledged. Similarly, hurricane induced storm surge flooding and high winds pose simultaneously occurring multiple hazards that can have a significant impact on not only the design of a nuclear plant but also on the accident management and emergency response.

Only a limited number of studies have been conducted to consider multi-hazard scenario in the design or risk-assessment. Ellingwood (2001) proposed a framework to calculate risk due to competing hazards based on total probability theorem. Subsequently, Ayyub et al. (2007) suggested the critical asset and portfolio risk analysis framework for evaluating risks under multiple hazards. Li and Ellingwood (2009) conducted multi-hazard risk assessment for wood-frame structures subjected to earthquake and hurricane. Beavers et al. (2009) studied the overall risk to bridges due to earthquakes, storm surge, and ship collision. Kameshwar and Padgett (2014) proposed a multi-hazard risk assessment for bridges subjected to earthquake and hurricane. The common theme in all these studies is that the risk is calculated for each individual hazard using the traditional approach wherein the hazard curve is convoluted with the fragility data. The effect of multiple hazards on the overall risk is computed by using the total probability theorem.

The fundamental assumption in using the total probability theorem is that individual hazards are statistically independent, mutually exclusive, and collectively exhaustive. Therefore, it cannot be used for assessment of risks associated with multi-hazard scenarios such as seismically induced internal flooding or flooding induced fires in which the undesirable response of the plant to one hazard acts as the initiator of another hazard making them correlated events. It can be argued that a well designed plant should not exhibit such failures. Traditional PRAs do not exhibit such correlated events because failures of these nature are not encountered in a plant that is well designed to withstand the design basis events. On the contrary, identifying and suppressing such events are the primary reason for the strong emphasis on evaluating vulnerability beyond design basis. The response of a plant's structures, systems, and components to beyond design basis events is quite different from that to the events at or below the design basis levels. Consequently, there is need for developing multi-hazard risk assessment methodologies to account for such correlated events beyond the design basis levels and to determine a plant's vulnerability. As additional studies are conducted and new data becomes available, such methodologies should allow easy and continued updating of plant risk.

A systems analysis is typically used to consider the various aspects mentioned above. Some of the typical tools used for conducting such systems analysis are fault tree analysis (FTA), event tree analysis, Petri net, PNET, logic tree, decision tree, etc. Out of these, a typical PRA in a nuclear power plant relies heavily on fault and event trees for modeling and assessment of system level failure. The system-level failure is typically referred to as the "top event (TE)." A fault-tree based approach can be broadly divided into two parts: (1) a qualitative development of the logic diagram which is then used to write an expression for the TE and determine the minimal cut-sets; (2) a quantitative evaluation based on probabilities of occurrence of basic events to determine the probability of occurrence of the TE (and of any intermediate-level events) together with a determination of the importance measure for each minimal cut-set. The importance measures are used to identify critical events contributing significantly to the probability of system failure and to identify the weak links. The limitations in the original implementation of the PRA have been improved in recent years (Mohaghegh et al., 2009). Bayesian updating has also been used within the existing PRA approaches for incorporating new information but the implementation and the influence of such updates on different components/events is not easy to visualize or interpret.

Certain limitations in the conventional PRA are generally overcome by combining it with other techniques or employing an alternative approach. For example, the uncertainties in basic event probabilities are considered by implementing an FTA in conjunction with Monte-Carlo simulation (Rasmussen, 1975) or Fuzzy set theory (Tanaka et al., 1983; Singer, 1990; etc.). The statistical dependencies between events are handled by introducing the correlation coefficients within a fault tree (Zhang, 1989; Fleming and Mikschl, 1999; Ebisawa et al., 2015). Consideration of the statistical correlations and relationships among events beyond what can be represented by logical gates is often handled by using FTA in conjunction with Event Trees (ET). Alternatively, the concept of Bayesian Network can also be employed but has not truly been utilized in the context of PRA. The concept of Bayesian Network was developed to directly manage various statistical dependencies. Bobbio et al. (2001) proposed the mapping method which converts a fault tree into a corresponding Bayesian network (BN). Such a network representation also facilitates a direct and simple implementation of Bayesian updating quite effectively for accommodating the new data/information (Hamada et al., 2004; Wilson and Huzurbazar, 2007; Kelly and Smith, 2009). Consequently, in this paper we explore the use of a Bayesian Network and Bayesian Inference based approach for multi-hazard risk assessment so as to account for statistical dependencies. The premise is to explore if this framework can allow identification of critical events for both the design basis risk as well as postulated "vulnerabilities." Illustrative examples are used to identify differences in possible solutions evaluated from the traditional approach compared to a Bayesian Network based risk assessment.

2. Summary of current PRA methodology

In the current methodology, the overall risk (i.e. annual probability of failure) for an individual hazard is evaluated by convolution of hazard curve and the corresponding fragility as following:

$$P_f = \int P_{f|\lambda} \cdot \left|\frac{dH(\lambda)}{d\lambda}\right| d\lambda \quad (1)$$

in which λ is a hazard intensity parameter, $P_{f|\lambda}$ is the fragility curve, and $H(\lambda)$ represents the hazard curve. The hazard curve expresses the probability of annual exceedance in a domain of the intensity measure used for characterizing the external hazard. The fragility curve for basic events is obtained by using empirical, experimental, and/or numerical simulation data. It represents the conditional probability of failure under each hazard's intensity. The system-level risk is calculated by employing either a series-parallel system as a simplistic representation of the complete system or by using logic trees. Furthermore, a complete PRA also considers random failure events that are not caused directly by external hazards. The random failure data is typically obtained from existing plant operational experience or other related research outcomes (USNRC, 1987; INEL, 1994; IAEA, 1997; EPRI, 1997). This failure data is in general represented as an annual failure rate. In the context of a multi-hazard risk assessment, risk estimates for different hazards