Progress in Nuclear Energy 105 (2018) 153–159

Contents lists available at ScienceDirect

Progress in Nuclear Energy

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

# Combined nuclear safety-security risk analysis methodology development and demonstration through a case study

Mohammad A. Hawila, Sunil S. Chirayath*

*Nuclear Engineering Department, Texas A&M University, College Station, TX 77843-3133, United States*

ARTICLE INFO

*Keywords:*
Combined risk analysis
Security-safety interface
SAPHIRE-code
Adversary sequence diagram

ABSTRACT

Destruction of critical nuclear infrastructure would have a debilitating effect on national public health, safety, national economy and security. For this reason, analysts perform safety risk analyses on the performance of the nuclear system to quantify and understand the nature of unwanted events. Since the world has gone through many changes after the terrorist attacks of 9/11, nuclear security risk analysis also became a necessity. To date, the safety and security risk analyses have been done separately without a combined evaluation. Study results are presented for three types of risk analyses for a pure security initiating event, pure safety initiating event, and a combined analysis of safety-security risk for either a security or safety initiating event. The pure security risk analysis uses adversary sequence diagram and pathway analysis to calculate the initiating security event frequency of a successful adversary attack. The pure safety analysis represented a series of natural (random) safety system component failure events for which a safety system failure frequency was calculated using SAPHIRE probabilistic risk analysis code. On the other hand, the combined safety-security analysis considered a security initiating event followed by safety system failure or vice versa. The main outcome of the comparative study of three different types of risk analyses is that pure safety risk evaluation without considering the possibility of a simultaneous security attack would underestimate the risk value. Failure frequency due to a security event should be combined with the safety system failure analysis for a meaningful risk analysis and the Estimate of Adversary Sequence Interruption (EASI) model can be employed for this purpose. The usefulness of a combined safety-security risk analysis is demonstrated through a case study for the spent fuel storage pool facility.

## 1. Introduction

Safety and security systems are generally an integral part of a nuclear fuel cycle facility. These systems are present in the facility to keep the risk to the public and the environment below an acceptable limit in the event of a safety or a security incident. Even before the safety and security systems are integrated into a facility it is important to analyze these system designs to draw conclusions on their performance potential and to identify vulnerabilities. These system design analyses are mostly performed through computational and simulation efforts to understand the system response to various initiating events (IEs) and determine System Failure Frequency (SFF). Individual Component Failure Frequency (CFF) data of the system is required to perform such a system design analysis.

Currently the SFF and the associated risk evaluations are separately done for nuclear safety and nuclear security systems, a brief description of which follows:

(1) Nuclear Safety Risk ($R_{SAF}$) evaluation is performed in three steps. First, calculate the SFF using a system representative fault tree and by employing the individual CFF data. The second step is to evaluate the radioactive source term resulting from the system failure and the third step is the estimation of the consequence in the public domain due to a partial or total release of radioactive source term to the environment (Bohn and Lambright, 1990). This methodology can be summarized in a simple equation as:

$$R_{SAF} = SFF_{SAF} \times C \quad (1)$$

Where, $SFF_{SAF}$ is the safety SFF and C is the consequence due to the radioactive source term released to the environment per system failure event (Helsby and White, 1985; Kirchsteiger, 1999).

(2) Nuclear Security Risk ($R_{SEC}$) evaluation is carried out by using the equation:

$$R_{SEC} = AAF \times (1 - P_I \times P_N) \times C \quad (2)$$

* Corresponding author.
*E-mail address:* sunilsc@tamu.edu (S.S. Chirayath).

https://doi.org/10.1016/j.pnucene.2018.01.005
Received 22 August 2017; Received in revised form 28 November 2017; Accepted 19 January 2018

Where, AAF is the Adversary Attack Frequency, $P_I$: is the probability of interruption of the adversary by the nuclear security system also known as the physical protection system (PPS), $P_N$: is the probability of neutralizing the adversary by the response force, and C is the consequence from the release of the radioactive source term from the successful adversary attack (Garcia, 2008). The term contained in brackets of equation (2) represents the probability of success ($P_S$) of the adversary, which when combined with AAF becomes the security SFF and will be designated as $SFF_{SEC}$. Hence equation (2) can be rewritten as:

$$R_{SEC} = SFF_{SEC} \times C \quad (3)$$

The consequence term, C in both equations (1) and (3) is the same no matter what triggered a system failure (safety or a security IE), since it similarly affects the public domain. Because of this common term, C, it is beneficial to develop a methodology that combines the safety-security risk evaluation. That is developing a combined risk evaluation methodology will be more optimal whether (a) IE is a security-type event (nonrandom event) followed by individual safety component failures (random failures) leading to a SFF or (b) IE is a safety-type event (random event) followed by security component failure (nonrandom event) leading to a SFF or (c) any combinations of (a) & (b) leading to a SFF. An example of a safety IE is the failure of a cooling pump used to remove process heat, which may lead to a chain of events affecting the heat removal system at the facility. An example of a security type IE is sabotage of the cooling pump by an adversary. Each of the IEs have its own IE frequency.

## 2. Objective of the study

The objective of the study presented here is to develop and demonstrate the benefits of employing a combined safety-security risk evaluation methodology as compared to the current method of calculating $R_{SAF}$ and $R_{SEC}$ independently as described in section 1. To demonstrate the methodology a typical nuclear Spent Fuel Storage Pool (SFSP) facility design shown in Fig. 1 is selected. To determine the benefits of the new methodology three evaluations (pure security risk, pure safety risk, and combined safety-security risk evaluations) are demonstrated for the case of the SFSP facility. The methodology demonstration considered both safety-type and security-type IEs. The most vulnerable path to the SFSP is analyzed completely from the security side to sabotage the entire cooling system; a full explanation can be found elsewhere (Hawila, 2016). Before describing the risk evaluations a brief discussion of the SFSP cooling system is inevitable, which is in following subsection.

### 2.1. SFSP cooling system function, components, and accident consequences

From lay out shown in Fig. 1 one can note that the SFSP cooling system consists of two parts: the primary cooling system, and the secondary cooling system. The primary cooling system has two main pumps that reflect system redundancy in which one pump works at a time during normal operation and the other is reserved for an emergency situation. One of the pumps draws coolant from the SFSP through a cooling pipe line, where two valves are installed on each pipe line to control the process. The primary cooling system also has a valve installed on the main pipe line (main valve) that controls the water withdrawal from the pool. Then water is passed through a heat exchanger system to extract the heat, and cool it down to be returned to the pool.

The secondary cooling system is composed of two pumps: a diesel driven pump and an electrical driven pump, which are installed over two independent pipelines to maintain independency and redundancy in the system. These pumps draw water from the reservoir and inject it into the SFSP during abnormal and accident conditions. The heat exchanger system extracts heat from the circulated cooling water and a small amount of water that passes through a filtration process.

Any possible accident at the SFSP, such as fire, a pipe breaking, pump failure, valve failure, component sabotage, etc., could lead to spent fuel melt and release of highly radioactive materials resulting in catastrophic consequences (Alvares, 2011). Thus, it is important to have reliable safety and security measures to ensure the functioning of both primary and secondary cooling systems at the SFSP. Now that, the SFSP cooling process and the importance of safety as well as security have been discussed in the following three sections describe the evaluation of pure security risk, pure safety risk and combined safety-security risk.

## 3. Pure security risk evaluation

Given the AAF (Chirayath, 2016) for the SFSP, the objective of the security risk evaluation is to calculate the $P_S$ of the adversary, which is $(1- P_I P_N)$ to defeat the PPS. Hence, AAF times $P_S$ will determine the CFF for primary and secondary cooling systems due to an adversary attack. The EASI (Estimate of Adversary Sequence Interruption) model is used to calculate the value of $P_I$ (Garcia, 2008). A Microsoft Excel macro worksheet is used to calculate $P_N$ (Snell, 2013).

### 3.1. Calculations of $P_I$ and $P_N$

This section presents the adversary pathway analysis to calculate $P_I$ and $P_N$. The analysis includes the movement of the adversary through multiple detection and delay elements of the PPS from offsite area to SFSP. The main two security concerns are theft (nuclear or radioactive materials) and sabotage (process or support equipment). For this study, the focus is on the sabotage case and the sabotage is to take out both primary and secondary SFSP cooling systems. Most vulnerable adversary path to the SFSP is analyzed and presented here, addressing the detection and delay elements of the PPS with their respective values of each element's probability of detection ($P_D$) and time delay ($t_D$). These elements and values lead to the calculation of the probability of interruption, $P_I$, which is one of the terms needed to assess the $P_S$ (refer to equation (2)). Another term needed for calculation $P_S$ is $P_N$. $P_N$ represents the result of response force engagement after interruption of the adversary. For the $P_N$ estimation, the adversaries' capabilities, tactics, and strength are required along with the state's neutralization strategy and measures. Data about the threat, response force, and PPS is required to analyze the engagements and estimate $P_N$. Data about the response force equipment also is needed such as: basic duty weapons, special duty weapons, intermediate force weapons, and vehicles.

Related to the $P_N$ estimation, the states' competent authority prepares a threat assessment document. This document contains information about the anticipated threats such as a terrorist group. This document works as the basis of defining the Design Basis Threat (DBT), which should consist of the attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal of nuclear material or sabotage, against which a nuclear security system is designed and evaluated. The neutralization analysis method used in this study is a simple numerical method, which uses an excel macro-calculator to determine $P_N$ (Snell, 2013).

The following assumptions were made on the adversary and response force capabilities. The adversaries are highly trained and have excellent tactics. Their attack plan is at night, and they are a group of 8. They have 7.62 mm semi-automatics, and 9 mm handguns, which are bladed. On the other hand, the response force has four teams of response, which are two armed guards, two men as tactical response, two snipers, and 12 men of offsite response. With these assumptions the value of $P_N$ obtained was 0.94. The final parameter that is needed to estimate the security risk value associated with SFSP sabotage using Equation (2) is the consequence (C) value. In this analysis, the sabotage