Annals of Nuclear Energy 99 (2017) 47–53

Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs)

Hyo Sung Cho [a], Tae Ho Woo [a,b,*]

[a] Department of Radiation Convergence Engineering, Yonsei University, 1 Yonseidae-gil, Wonju, Gangwon-do 26493, Republic of Korea
[b] Department of Mechanical and Control Engineering, The Cyber University of Korea, 106 Bukchon-ro, Jongno-gu, Seoul 03051, Republic of Korea

ARTICLE INFO

Article history:
Received 9 April 2015
Received in revised form 9 September 2016
Accepted 14 September 2016

Keywords:
Nuclear power plants
Cyber security
Terrorism
Safety

ABSTRACT

The cyber terrorism for nuclear power plants (NPPs) is investigated for the analytic study following the South Korean case on December 2014. There are several possible cyber terror attacks in which the twelve cases are studied for the nuclear terror cases including the computer hacking and data stealing. The defense-in-depth concept is compared for cyber terrorism, which was imported from the physical terror analysis. The conventional three conditions of the physical protection system (PPS) are modified as prevention, detection, and response. The six cases are introduced for the solutions of the facility against the possible cyber terrorism in NPPs. The computer hacking methods and related solutions are analyzed for the applications in the nuclear industry. The nuclear security in the NPPs could be an extremely serious condition and the remedies are very important in the safe plant operations. In addition, the quantitative modeling study is performed.

1. Introduction

The nuclear terrorism has been concerned extensively following the nuclear safety. The cyber terror in the nuclear power plants (NPPs) produced many security issues from the incident which had happened on December 2014 in South Korea (Republic of Korea) (ABC, 2014; BBC, 2014; Cho, 2014; Woo and Kwak, 2015). Considering of increasing trend in terrors, the attacking on nuclear facility has one of serious situations. In the attack, it was requested that unless three reactors were closed by Christmas, people should stay away from them (BBC, 2014; Woo and Kwak, 2015). However, there was not any attack on the NPPs and other nuclear facilities in South Korea. So, this paper would like to investigate the cyber terror attacks and the related matters including the protection protocols. Furthermore, recently (March 12th) the hacker asked for the money revealing the some plant drawings and the phone conversation record between Korean president and the United Nations Secretary-General (YTN, 2015). Table 1 shows the three stages of cyber terror attack on the Korea Hydro & Nuclear Power Co. Ltd. (KHNP) (VOA, 2015; Kimb, 2015). Fig. 1 is the simplified networking system for KHNP where the reactor and internal systems are disconnected from the external system (KHNP, 2014). The geological sites of NPPs are seen in the map on Fig. 2 in which the sites are located on the south east region in Korea (NGII, 2015).

Cyber terrorism in NPPs is considered as the computer-based internet terrorism as well as the nuclear terrorism in which the potential damages could be considered. In the case of cyber terror, the psychological concerns are very higher comparing to any other physical terrors. Hence, the economic damages could increase such as the stagnations of the economic activity. As a matter of fact, the employee had suffered from the maximized alert condition during all Christmas day long. The normal life cycle of the person or other scheduled tasks were delayed or cancelled in order to concentrate on the preparations against the possible terror attacks.

2. Literature review

There are several computer virus infection incidents in NPPs which could be similar effects like the cyber terrorism on NPPs. The Microsoft SQL Slammer worm was infected on the Davis-Base NPP in 2003 (US NRC, 2003; Kim, 2014). The excessive traffic in the plant's integrated computer system network had failed the recirculation pump variable frequency drive (VFD) controllers and the condensate demineralizer controller, equipped with the dual redundant programmable logic controller (PLC) system connected to the integrated computer system network on Browns Ferry in 2006 (US NRC, 2007; Kim, 2014). In addition, the Stuxnet

* Corresponding author at: Department of Mechanical and Control Engineering, The Cyber University of Korea, 106 Bukchon-ro, Jongno-gu, Seoul 03051, Republic of Korea.
E-mail addresses: thwoo@cuk.edu, thw_kor@hotmail.com (T.H. Woo).

http://dx.doi.org/10.1016/j.anucene.2016.09.024
0306-4549/

Table 1
Stages of cyber terror attack on Korea Hydro & Nuclear Power Co. Ltd. (KHNP) (VOA, 2015; Kimb, 2015).

Stage	Content
1	Data leaks by hacker in Shenyang, China Method – Direct connection – Virtual Private Network (VPN) Used software – Retired employee's ID – Fishing mail – Virus codes Data – Personal information of employees – Contents and account of emails – Internal PC
2	Emailing to KHNP employees (about 6000) with the virus code (Dec. 9, 2014). But, attack failed Method – Virtual Private Network (VPN)
3	Data opened and threatened Method – Direct connection – Virtual Private Network (VPN)

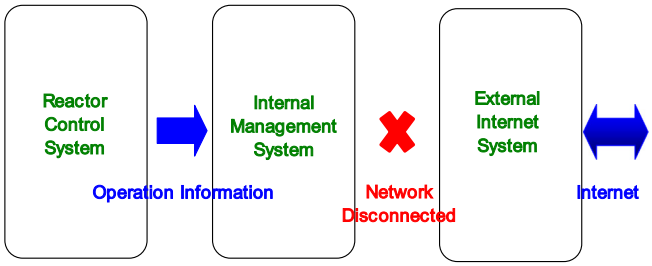

Fig. 1. Simplified networking system for KHNP.

computer worm was identified by a Belarus-based security firm (Virus-BlokAda) where Stuxnet is a serious computer virus in the NPPs (Dagouat, 2011; Kim, 2014).

Regarding the related research, the United State Department of Energy studied the cyber security in the nuclear facility for nuclear regulatory guide 5.71 (US NRC, 2010) where Title 10, of the Code of Federal Regulations, Section 73.54, "Protection of Digital Computer and Communication Systems and Networks" (10 CFR 73.54) (Ref. 1) requires, in part, that U.S. Nuclear Regulatory Commission (US NRC) licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat (DBT), as described in 10 CFR 73.1, "Purpose and Scope."

There was the general analysis of the nuclear terror where eight cases are studied as the potential terror incidents in the commercialized NPPs (Woo, 2013a). Cipollaro and Lomonaco studied for the nuclear safety, nuclear security and nuclear safeguards (Cipollaroa and Lomonacob, 2016). Jakopič et al. studied for the quantitative verification by independent measurements (Jakopič et al., 2013). Zakariya and Kahn worked for several approaches in the design of physical protection system (PPS) (Zakariya and Kahn, 2015). In addition, there were several assessment and forecasting studies incorporated with the protection ideas (Woo and Lee, 2010, 2011a,b,c; Woo, 2011, 2012, 2013b, 2015; Woo and Kim, 2012). Shin et al. studied the nuclear cyber security issue where a risk model is based on a Bayesian network for nuclear facilities in an integrated manner (Shin et al., 2015). In addition, Silva et al. worked for making interactions in the virtual environment in which the nuclear facility structure could be simulated to give the planning action strategies to enhance its security (da Silva et al., 2015).

3. Method

The comparisons between general and cyber terror cases are shown in Table 2 where several characteristics are analyzed.

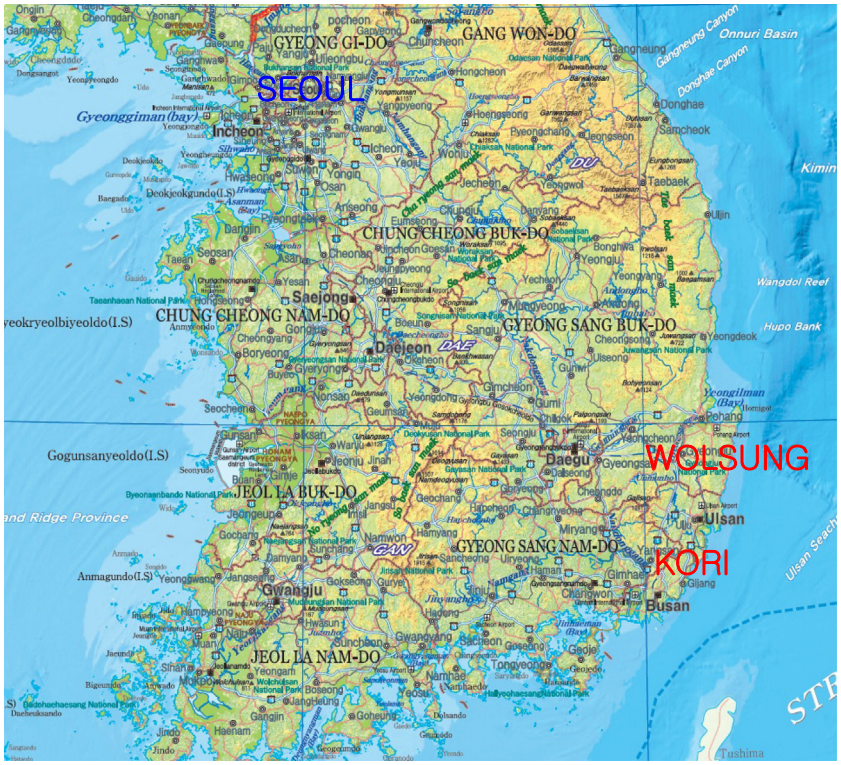

Fig. 2. Map of South Korea.