On the Recent Research Advancements of Cyber Security of Nuclear Power Plants

Yan-Fu Li[a], Shou-Zhou Liu[a]
[a] Department of Industrial Engineering, Tsinghua University, Beijing, China

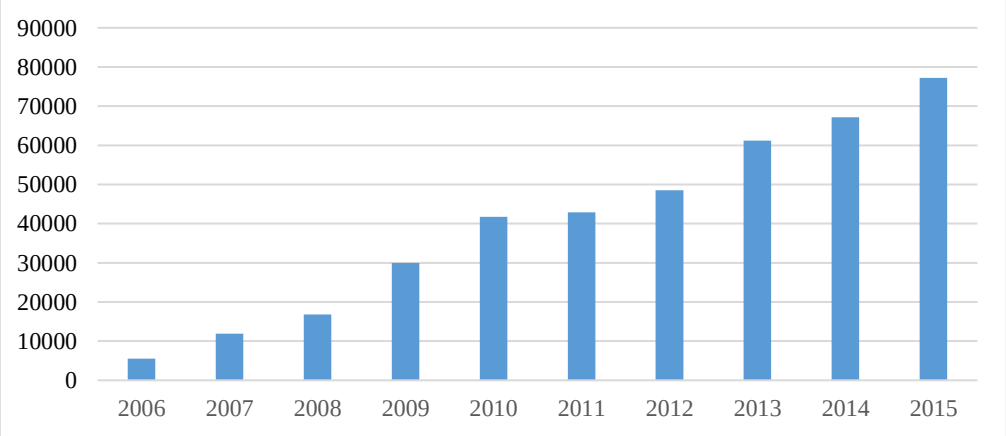
Abstract: In recent years, human society has observed a world-widely increasing number of cyber-attacks, with increasing complexities, applied onto different information, telecommunication and control (ITC) systems including those in the nuclear power plants (NPPs). The target of those attacks against NPPs can be various subsystems of instrumental and control (I&C) systems, e.g. reactor protection systems, engineering workstations, etc. In response to the rising threats from the cyber space, regulations and technologies have been and are being developed to protect and enhance the cyber-security of I&C systems. Recently, a number of regulations and standards have been made for the prevention and mitigation of cyber threats. Meanwhile, an increasing number of research works have been published with the focuses on cyber-security assessment and protection To understand what are the cyber-attacks, how are they implemented, what are their consequences, how to analyze, assess and predict the cyber threats as well as what are the protection mechanisms, what are the optimal ways of deploy them, are beneficial to both researchers and practitioners. In this paper, we will deliver a state-of-the-art overview on various aspects of the cyber-security of NPP.

Keywords: Cyber Security, cyber-attack, risk, nuclear power plant.

1. INTRODUCTION

In recent years, with the prevalent installation of information and communication devices the man-made engineering systems have undergone a transform from the conventional physical systems to the more complex cyber-physical systems. Along this trend, human society has observed a world-wide increasing of cyber-attacks, applied onto different information, telecommunication and control (ITC) systems. One piece of the evidence is in Figure 1, which shows that the number of cyber-attacks reported by the federal agencies in the U.S. steadily increases during the period of 2006 – 2015. Given the rapid growth of latest information technologies, e.g. internet of things (IoT) and artificial intelligence (AI), it is not surprising to conject that this trend will continue from 2016 onwards.

Figure 1: Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2015 [1]

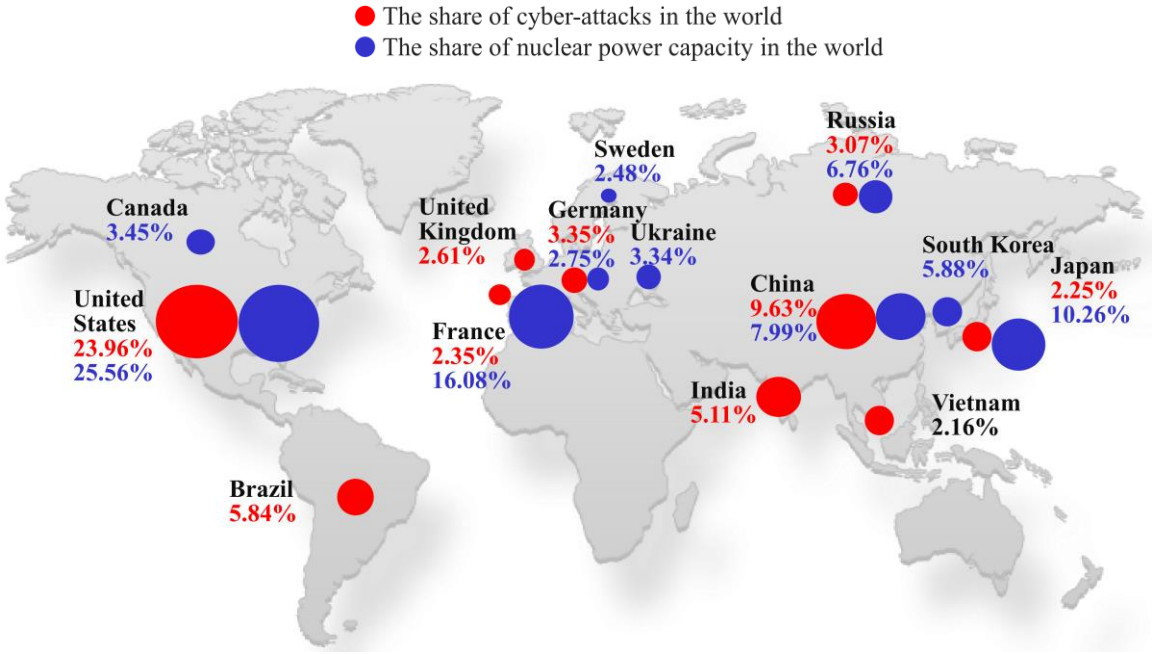


The Fukushima accident in 2011 has retarded the global nuclear energy development for a few years. But, nuclear, as a clean, reliable and cost-effective energy, has attracted a large number of countries,

especially China and other developing countries, continuously boosting NPP construction projects. According to the '2017 report of international status and prospects for nuclear power' by International Atomic Energy Agency (IAEA) [2], the countries that are really against nuclear is the minority and global nuclear power capacity installation indicates an increase from the 2016 level by 123% in 2050 at the high case and an retention of the 2016 level in 2050 at the low case.

Given the promising future of nuclear energy, the world-wide presence of many NPPs will be enduring and significant. According to IAEA [3], in 2016 the top 10 countries of nuclear power capacities are the U.S., France, Japan, China, Russia, South Korea, Canada, Ukraine, Germany and Sweden. On the other hand, the increasing cyber-attacks can be a constant threat to the NPPs. According to the software security company Symantec, the top 10 source countries of cyber-attacks in 2016 are the U.S., China, Brazil, India, Germany, Russia, U.K., France, Japan and Vietnam. As shown in Figure 2, there are obvious overlaps between these two groups, e.g. the U.S. and China both have significant proportions of nuclear capacities and cyber-attacks. Given the borderless property of internet, international cyber-attacks to the NPPs in other countries are also possible.

Figure 2: Collocation of World Major Cyber-attacks Sources and Nuclear Energy Capacities

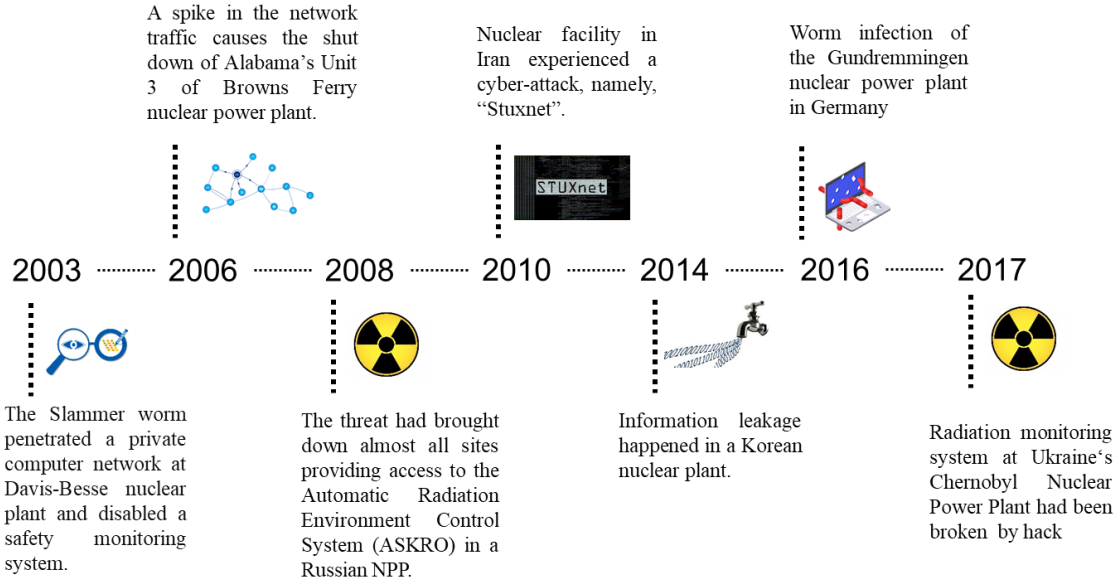


In fact, several cyber-attacks against NPPs or other nuclear facilities had already happened in recent years. Figure 3 exhibits a series of major attack events in chronological order from 2003. These attacks typically damage the instrumentation and control (I&C) systems in NPP via personal computers or business network. By conducting these attacks, the hacker normally halt the normal operation of NPP and cause financial damage to NPP operators. Following are the brief descriptions of these accidents.

- In 2003, the Slammer worm penetrated a private computer network at Ohio's idled Davis-Besse NPP and disabled a safety monitoring system for nearly five hours. This worm entered the plant network through an interconnected contractor's network, bypassing Davis-Besse's firewall [4].
- In 2006, a spike in the data traffic caused the shutdown of Unit 3 of Browns Ferry NPP at Alabama. During this accident, a deluge of data has locked up the controllers of two water recirculation pumps such that the operator has to shut down the reactor after the failures of the recirculation pumps [5].
- In 2008, the hackers attacked the websites of Leningrad NPP which provides information about the background radiation levels in order to issue false alarms of a nuclear accident. This was a planned action which brought down almost all websites providing access to the Automatic Radiation Environment Control System (ASKRO) [6].

- In 2010, over fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. It was believed that this attack was initiated by a random worker's USB drive. One of the affected industrial facilities was the Natanz nuclear facility [7].
- In 2014, Korea Hydro & Nuclear Power (or KHNP) officially announced that its computer systems had been hacked. The group that hacked KHNP's server gained access to some plant computers and released stolen blueprints of nuclear reactor, details on various support systems and personal data of over 10,000 employees. The hackers also posted on their Twitter stating that "Unless you stop operating the nuclear power plants until Christmas and give us $10 billion, we will continue to release the secret data related to the facility" [8].
- In 2016, several computer viruses had been detected in a German nuclear power plant in Bavaria. The malware could steal login credentials and allow a remote attacker to access the cracked computer [9].
- In 2017, Ukraine's crucial infrastructures, e.g. national bank, state power company and largest airport were under large scale cyber-attacks. The attacks also stroked the radiation monitoring system at Ukraine's old Chernobyl NPP, which has been broken to offline status, forcing the employees to use hand-held counters to measure radiation levels [10].

Figure 3: Recent Major Cyber-Attack Events Targeting Nuclear Facilities



The nuclear energy industry began addressing cyber security immediately after the terrorist attacks of Sep. 11, 2001. To the knowledge of the authors, this is the first overview on NPP cyber security research works in recent years. The rest of this paper is organized as follows. Section 2 briefly reviews the I&C systems and the cyber-attacks applied to NPPs. Section 3 surveys the research publications on NPP cyber security between 2011 and 2017. Section 4 concludes this work and presents discussions about the future research directions.

2. CYBER-ATTACKS TO NPP

The NPP is a complex system consisting of various subsystems, such as nuclear reactor, heat transport system, steam generators, electrical generator, power transmission, etc., which resemble the physical parts of the NPP. The I&C system, on the other hand, is the cyber part of the NPP. Together with the operation personnel, I&C system severs as the "central nervous system" of a plant. Therefore, most cyber-attacks onto NPP are aiming at its I&C system.

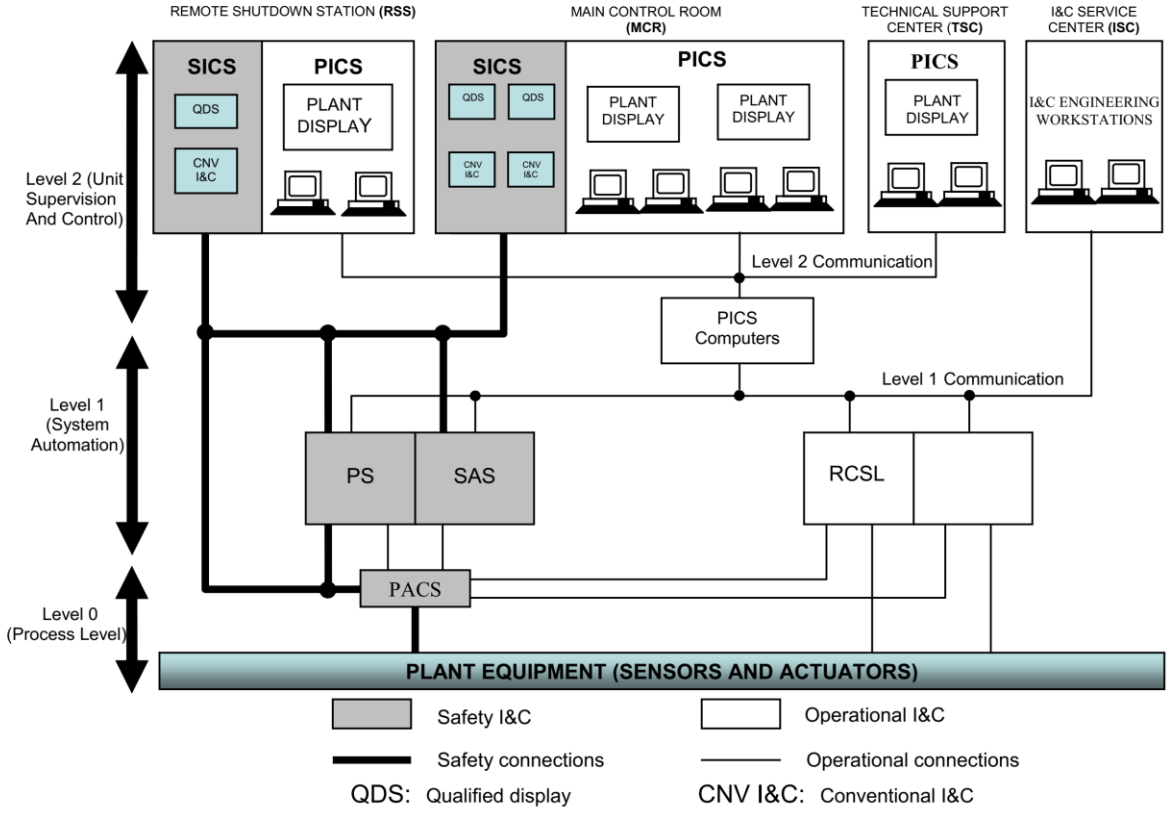
2.1. Instrumentation and Control System

The I&C system is mainly responsible for the reliable operation of a NPP. In general, NPP is operating under normal condition when several key parameters, e.g. pressure, temperature, power and flow rate, are controlled within the design limits, through the functioning of numerous electromechanical components, e.g. pumps, motors and valves. The coordination of all these components are realized by the different elements of I&C system. They sense process parameters, estimate deviations/abruptions, monitor performance, integrate information, issue corrective actions to failed components and make automatic adjustments to plant operations as necessary [11]. They also send messages to and receive responses from a human-machine interface (HMI) to support operators during accidents [12].

The architecture of I&C system consists of several levels. In this paper, we briefly present the European Pressurized Reactor (EPR) (the U.S. version is called the Evolutionary Pressurized Reactor or US-EPR) I&C system architecture (shown in Figure 4), which has the following three levels [11]:

- **Level 0 - process interface level** forms the physical interface between Level 1 systems and sensors, actuators and switchgears. The measurements of this level are sent to Level 1 systems, which compare them with defined value and take corrective actions, if necessary.
- **Level 1 – system automation level** consists of protection system (PS), safety automation system (SAS), process automation system (PAS), priority actuation and control system (PACS) and reactor control, surveillance, and limitation (RCSL) system. These systems automatically control the devices of the main plant and ancillary systems, based on the inputs received from sensors.
- **Level 2 – unit supervision and control level** consists of the workstations and panels of the main control room (MCR), remote shutdown station (RSS), technical support center (TSC), process information and control system (PICS) and safety information and control system (SICS). This level is responsible for the interactions between the operators and the rest of the systems at levels 1 and 0.

Figure 4: Architecture of the I&C System in US-EPR Plants [11]



2.2. Cyber-Attacks

In general, the cyber-attacks can be roughly classified into three types: attacks against available of service, attacks against data integrity and attacks against confidentiality [13]. The first type is also called availability attacks. They mainly consist of denial of service (DoS) attacks and distributed denial-of-service (DDoS). DoS attacks generally attempt to delay, block or corrupt the legal communications, make it unavailability to the authorized parties. Integrity attacks aim at modifying or disrupting data exchange in the communication system. Man-in-the-middle (MITM) attack and replay attack belong to this type of attacks. The target can be various subsystems of I&C, e.g. reactor protection systems, engineering workstations, etc. Attacks against confidentiality can cause information disclosure to unauthorized parties. These attacks can be implemented by guessing password or port scanning. Different attacks are often combined in order to achieve certain objectives.

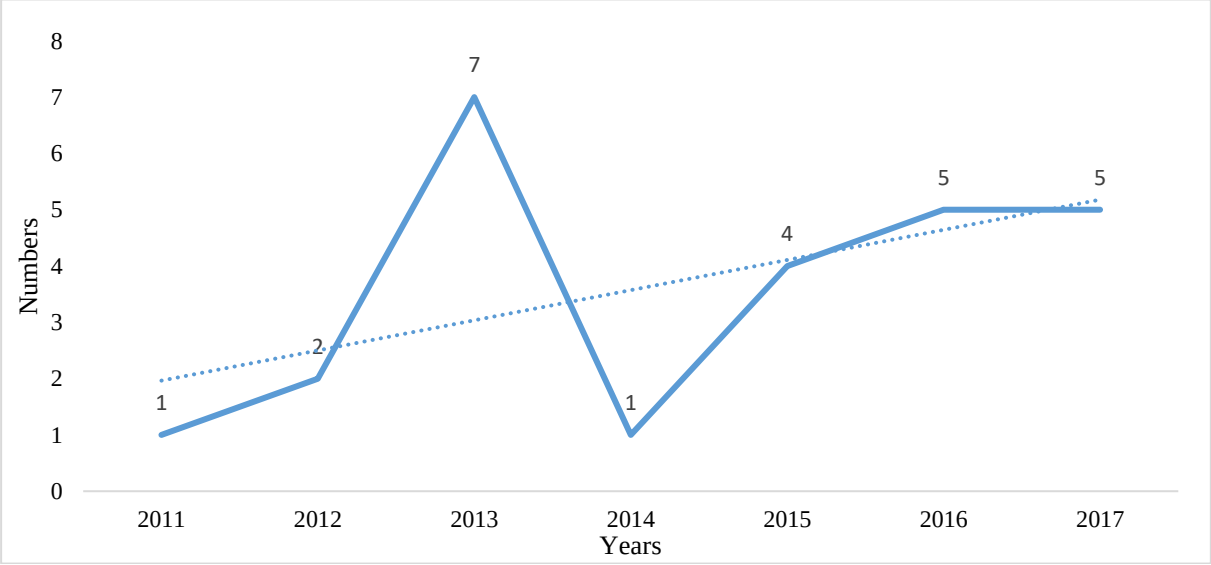
Most real-world cyber-attack events can be grouped into one of the above three types. Take the Davis-Besse NPP accident for example. The Slammer worm intruded from a business consultant's network to the NPP operating company's network and then get into the I&C network of the plant. It generated malicious traffic that jammed the NPP company and I&C networks. For almost five hours, plant employees were unable to access the safety parameter display system. This is a DoS type of attack that against availability.

3. REVIEW ON RECENT RESEARCH WORKS

Cyber security is not a completely new topic in nuclear field. In respond to the rising threats from the cyber space, recently a number of regulations and standards have been made for the prevention and mitigation of cyber threats [9, 14, 15]. Meanwhile, an increasing number of research works have been published with the focuses on cyber-security protection and cyber security risk assessment.

We have conducted a survey in the Web of Science database for the relevant publications from 2011 to 2017, using the combinations of the following keywords: cyber security, nuclear plant, cyber-attack, instrumentation and control system, risk assessment, cyber security strategy. Figure 5 shows the number of publications each year. It is observed that the amount of research works is steadily increasing.

Figure 5: Numbers of Publications Relevant to NPP Cyber Security from Web of Science Database in the Period 2011-2017



According to the main purpose of the studies, we have classified them into three main categories: cyber security defense, cyber security assessment and others. The category 'others' includes the publications that mainly digest and interpret the regulations and standards.

3.1. Cyber Security Protection

The studies under this group focus on various aspects of the protection of NPP cyber security, including mainly the design or deployment of critical digital assets (CDA) architecture against cyber threats and the development of abnormality detection method for the potential cyber-attacks against specific I&C equipment.

Many design studies are based on the defense-in-depth conceptual approach for cyber security defensive architecture deployment defined in NRC Regulatory Guide 5.71 [15]. In this approach, the CDAs are first identified then the defensive strategies are applied on them according to their ranks. This defensive architecture includes five levels separated by security boundaries, such as firewalls and diodes, at which digital communications are monitored and restricted. Systems requiring the greatest degree of security are located within a greater number of boundaries.

Miao [16] studied the deployment of the hardware-based information security technologies to realize defense-in-depth architecture to ensure the reliability and security of Chinese NPP. Son and Kim [17] applied the defense-in-depth concept for the design of multi-server architecture in NPP. Due to the incompatibility of the general regulations and standards to the research reactor facilities, Park et al. [18] developed a graded approach for the cyber security of research reactors and introduced cyber security activities for guarding the digital systems of research reactors. Bajramovic and Gupta [19] suggested that the newcomer countries must consider Design Basis Threat (DBT) as one of the security fundamentals during the design phase of the physical and cyber protection systems and multiple DBT scenarios need to be included to protect various target materials and facilities.

Different I&C subsystems can be the targets of different cyber-attacks, thus their cyber securities have to be specifically ensured. The operator display used for supporting software controlled automated systems belongs to critical infrastructures. Cyber-attacks that could modify the operator display is an important threat to NPP operation, Horowitz and Pierce [20] proposed to couple diversely redundant security designs with system dynamics models and state estimation techniques for the detection of the intentional adjustments to operator displays. The operating SCADA systems generate large number of log files, which are useful in analysis of the plant behavior and diagnostics during an ongoing attack, thus Gawand et al. [21] focused on such data and developed an effective monitoring scheme against the control aware cyber-attacks applied onto SCADA systems.

3.2. Cyber Security Risk Assessment

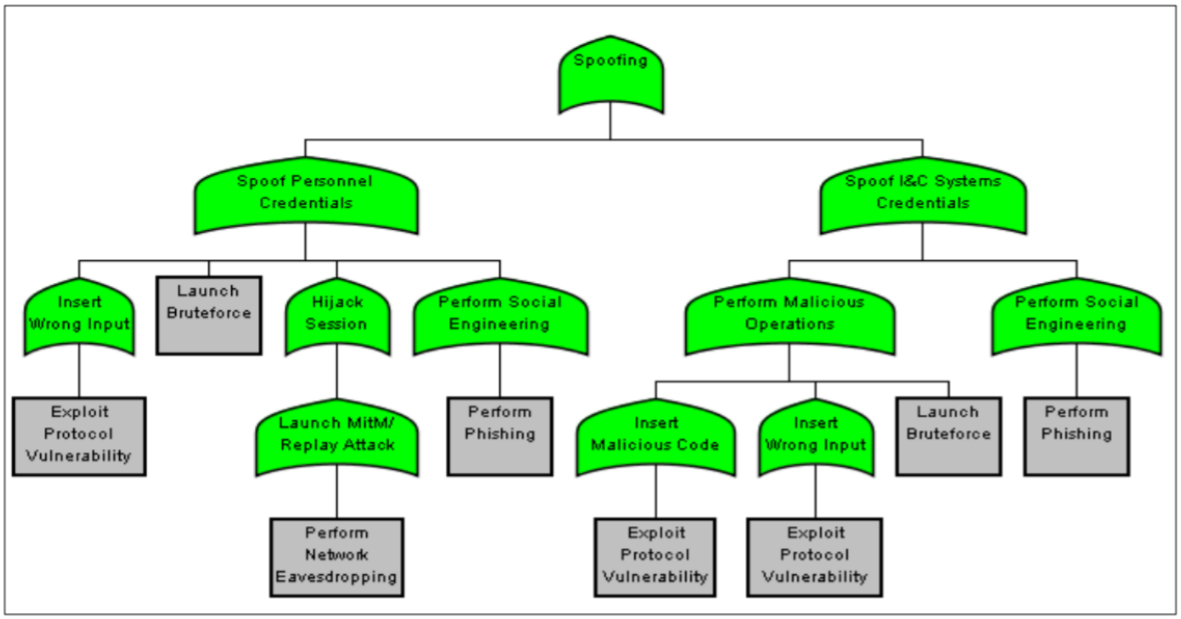
Given the high security requirement of NPPs, it is often difficult to conduct penetration experiments on running NPPs to obtain data for cyber security risk assessment. Alternatively, Shin et al. [22] proposed a Bayesian network approach that makes use of prior information, posterior information and backpropagation calculation. This model is reported to enable the evaluation of both the procedural and technical aspects of cyber security, which are compliant with regulatory guides and system architectures, respectively. Later on, Shin et al. [23] integrated the Bayesian network into the event tree model to build a probabilistic safety assessment (PSA) framework for nuclear facility cyber security.

Based on the basic understanding of NPP I&C systems, Song et al. [24] proposed a comprehensive assessment process for the design of such systems, which includes system identification, security modeling, threat analysis, penetration tests, etc. Through this process, potential system vulnerabilities and protection measures can be identified. More effective risk assessment needs to consider the event initiator: attackers. From the perspectives of attackers, an attack vector (i.e. attack path) is a set of vulnerable CDA components including human elements that need to be compromised/malfunctioned for achieving the attack goals. Song et al. [25] investigated the possible attack vectors for vulnerability identification and penetration tests on a simplified safety system, then appropriate cyber security requirements and technical security controls from RG 5.71 are selected and applied based on the results of the assessment.

One extension of the attack vector is the attack tree approach introduced in [12]. Attack trees have a hierarchical representation, in which the higher-level attack goals are broken down into sub-goals, until the desired refinement level is achieved. Attack trees are suitable for NPP cyber security assessment mainly due to the following reasons: I) they describe the steps of a successful attack in a more structured way than natural language; II) the model of an attack tree is illustrative and easy for comprehension; III) quantitative modeling and analysis can be performed upon the attack trees. A special notation is given here to the potential development of analytical approach that employs the mathematical modelling of the dynamic behaviors of the attackers and defenders, i.e. game theoretical modelling, based on the comprehensive analysis using the attack tree. Another way of accounting for the dynamics is presented by Woo [26]. This work applied nonlinear dynamic algorithm for the assessment of NPP security. Some observations and suggestions were made out from the quantitative simulation study developed with the systems thinking.

Different from the studies above, Slayton [27] performed an empirical cost-benefit analysis of the Stuxnet cyber-attacks on Iran's nuclear facilities which shows that these attacks very likely cost the offense much more than the defense. However, the perceived benefits of both the Stuxnet offense and defense were likely two orders of magnitude greater than the perceived costs, making it unlikely that decision makers focused on costs. The cost-benefit analysis is inspiring to the futuristic game theoretical modeling of the attack-defense behaviors in the context of NPP I&C systems.

Figure 6: Example of One Attack Tree of the Spoofing Attack [12]



4. CONCLUSIONS AND DISCUSSIONS

To understand what are the cyber-attacks, how are they implemented, what are their consequences, how to analyze, assess and even predict the cyber threats, what are the protection mechanisms, what are the optimal ways of deploying them, are beneficial to both researchers and practitioners. In this paper, we delivered a state-of-the-art overview on the above aspects of the cyber-security of NPP in recent years. The outcomes of this review indicate some potential directions for future research: 1) empirical research as such intrusion detection and anomaly detection techniques can be performed for NPPs ; 2) quantitative risk assessment methods would be developed to facilitate the design and deployment of defensive mechanisms; 3) proactive and dynamic defensive mechanisms can be considered for preventing potential threats.

REFERENCES

[1] Statistica. (April 2, 2018). *Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2015*. Available: https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/

[2] IAEA, "International Status and Prospects for Nuclear Power 2017," 28 July 2017.

[3] IAEA. (19 April 2017). *Nuclear Share of Electricity Generation in 2016*.

[4] K. Poulsen, "Slammer worm crashed Ohio nuke plant net," *The Register,* vol. 20, 2003.

[5] R. Lemos, "Data storm" blamed for nuclear plant shutdown," *SecurityFocus, May,* vol. 18, p. 84, 2007.

[6] J. Carr and S. Goel, "Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats," *Grey Logic, January,* vol. 21, 2010.

[7] M. Holloway, "Stuxnet Worm Attack on Iranian Nuclear Facilities," *Retrieved April,* vol. 13, p. 2017, 2015.

[8] J. Min, "North Korea's Asymmetric Attack on South Korea's Nuclear Power Plants."

[9] A. Lochthofen and D. Sommer, "Implementation of computer security at nuclear facilities in Germany," *Progress in Nuclear Energy,* vol. 84, pp. 103-107, 2015.

[10] N. Perlroth, M. Scott, and S. Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally," *The New York Times,* 2017.

[11] K. Korsah, D. E. Holcomb, M. D. Muhlheim, and J. A. Mullens, "Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update," U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington DC,NUREG/CR-6992, 2009, Available: http://www.nrc.gov/docs/ML0929/ML092950511.pdf, Accessed on: April 2, 2018.

[12] R. Masood, "Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives," Cyber Security and Privacy Research Institute, George Washington University GW-CSPRI-2016-03, 2016.

[13] D. Tellbach and Y. F. Li, "A survey on the cyber-security of distributed generation systems," in *27th European Safety and Reliability Conference (ESREL 2017)*, Portoroz, Slovenia, 2017, p. 14: CRC Press.

[14] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," *NIST special publication,* vol. 800, no. 82, pp. 16-16, 2011.

[15] NRC, "Regulatory Guide 5.71: Cyber security programs for nuclear facilities. ," US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2010.

[16] X. Miao, "Adopting Defence-in-depth Architecture, Ensuring the Reliability and Security of Nuclear Power [J]," *Process Automation Instrumentation,* vol. 2, p. 000, 2011.

[17] H. Son and S. Kim, "Defense–in–Depth Strategy for Smart Service Sever Cyber Security," in *Computer Applications for Communication, Networking, and Digital Contents*: Springer, 2012, pp. 181-188.

[18] J. Park, J. Park, and Y. Kim, "A graded approach to cyber security in a research reactor facility," *Progress in Nuclear Energy,* vol. 65, pp. 81-87, 2013.

[19] E. Bajramovic and D. Gupta, "Providing security assurance in line with national DBT assumptions," in *AIP Conference Proceedings*, 2017, vol. 1799, no. 1, p. 050005: AIP Publishing.

[20] B. M. Horowitz and K. M. Pierce, "The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems," *Systems Engineering*, vol. 16, no. 4, pp. 401-412, 2013.
[21] H. L. Gawand, A. Bhattacharjee, and K. Roy, "Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach," *Nuclear Engineering and Technology*, vol. 49, no. 3, pp. 484-494, 2017.
[22] J. Shin, H. Son, and G. Heo, "Development of a cyber security risk model using Bayesian networks," *Reliability Engineering & System Safety*, vol. 134, pp. 208-217, 2015.
[23] J. Shin, H. Son, and G. Heo, "Cyber security risk evaluation of a nuclear I&C using BN and ET," *Nuclear Engineering and Technology*, vol. 49, no. 3, pp. 517-524, 2017.
[24] J.-G. Song, J.-W. Lee, C.-K. Lee, K.-C. Kwon, and D.-Y. Lee, "A cyber security risk assessment for the design of I&C systems in nuclear power plants," *Nuclear Engineering and Technology*, vol. 44, no. 8, pp. 919-928, 2012.
[25] J.-G. Song, J.-W. Lee, G.-Y. Park, K.-C. Kwon, D.-Y. Lee, and C.-K. Lee, "An analysis of technical security control requirements for digital I&C systems in nuclear power plants," *Nuclear Engineering and Technology*, vol. 45, no. 5, pp. 637-652, 2013.
[26] T. H. Woo, "Systems thinking safety analysis: nuclear security assessment of physical protection system in nuclear power plants," *Science and Technology of Nuclear Installations*, vol. 2013, 2013.
[27] R. Slayton, "What is the cyber offense-defense balance? Conceptions, causes, and assessment," *International Security*, vol. 41, no. 3, pp. 72-109, 2017.