# Guarini Institute for Government and Leadership
# Saint Peter's University

## White Paper Series
## 2015 – 2016

## Preface

The Guarini Institute for Government and Leadership White Paper Series (GWPS) is designed to stimulate timely and relevant discussion around key public policy topics germane to New Jersey. The series will provide contributors a unique opportunity to share their opinions related to critical public policy issues that impact New Jersey communities and citizens. *The position/argument reflects that of the author and not Saint Peter's University or the Guarini Institute. Additionally, this paper cannot be reprinted without the consent of the Institute's Executive Director.*

Leila Sadeghi, Ph.D.
Executive Director
Guarini Institute for Government and Leadership
Saint Peter's University

## About the Author

Edward Moskal, MS, MMS, is the Chair of the Department of Computer and Information Sciences. Professor Moskal has been teaching at Saint Peter's University for the past 13 years and recently completed a one year Fellowship at the University of Notre Dame, where he worked in the Department of Computer Science and Engineering designing a Cyber Security Center and developing and teaching new graduate courses in Cyber Security and Digital Forensics. His research interests include Cyber Security and Data Science. Prior to coming to Saint Peter's, Professor Moskal worked in the Information Technology industry for 25 years. His last position in industry was with Ernst & Young where he worked in a Senior Management capacity leading the New York Office Application Controls and Security Practice. Client engagements included performing a Risk Assessment for the New York Stock Exchange, designing and implementing a Global Security Architecture for American Express, and designing the Security Architecture and Computer System Controls for the MTA E-ZPass System.

Professor Moskal can be reached at: emoskal@saintpeters.edu.

# Cyber Attacks on Nuclear Power Plants in New Jersey
# What are the Vulnerabilities? What can be Done?

## Introduction

There is a growing concern that a cyber-attack will hit one of the sixteen United States' critical infrastructure sectors, and the nuclear power plants in New Jersey are categorized in one of the sixteen sectors, particularly the Nuclear Industry sector. The Nuclear industry sector assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, the national economy, public health and safety. This paper discusses nuclear power plant concerns, design, and vulnerabilities, and the role of the Nuclear Regulatory Commission. It describes how a computer worm can sabotage a nuclear power plant and highlights recommendations for what the state of New Jersey can do to mitigate risk and help ensure that cyber-attacks are both prevented and deterred.

## The Problem: Nuclear Power Plant Concerns

Many nuclear power plants around the world are not well prepared to defend against cyber-attacks, according to a report titled "Cyber Security at Civil Nuclear Power Plants," published by Chatham House in September 2015. Chatham House, the Royal Institute of International Affairs, is an independent policy institute based in London that engages governments, the private sector, civil society and its members in debate and discussion on significant developments in international affairs. Researchers in the report studied cyber defenses in nuclear plants worldwide for 18 months and concluded that plant infrastructure was "insecure by design" because of their age. Digital systems have been adopted later in the nuclear industry than in other sectors. The industry's focus has also been on physical security and safety, which means less focus has been on cybersecurity. [1]

The International Atomic Energy Agency (IAEA) has announced a warning, which has urged the world community to intensify efforts to protect nuclear facilities from possible cyber-attacks. Pointing out the nuclear industry was not immune to such attacks, the IAEA Director, stated "there should be a serious attempt at protecting nuclear and radioactive material" since reports of actual or attempted cyber-attacks are now virtually a daily occurrence. [2] The Director at the Stockholm International Peace Research Institute stated, "Any corruption, malware or targeted attacks potentially could have catastrophic consequences for nuclear safety and security". [3]

On a daily basis, as hackers continue to rifle-through closely guarded networks, servers, databases, and information systems, there is a tempting new target for cyber-attacks: the world's nuclear facilities and we have three nuclear power plants right here in New Jersey. A good resource that illustrates the cyber-attacks that are taking place real-time, world-wide, is the NORSE Cyber Attack Map. This Map

[1] https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks
[2] http://www.ipsnews.net/2015/08/worlds-nuclear-facilities-vulnerable-to-cyber-attacks/
[3] Ibid.

shows the origin of the cyber-attack, the attack target, as well associated information on the Internet address and type of attack.

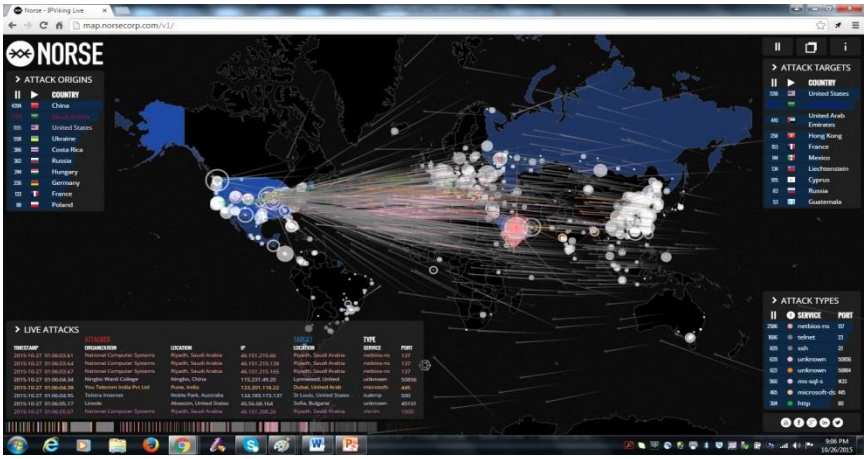


Figure 1 – NORSE Cyber Attack Map[4]

## Nuclear Power Plant Systems

Nuclear facilities use digital and analog systems to monitor and operate equipment. Analog systems perform operations by following "hard-wired" instructions, while digital systems (computer-based) follow instructions stored in memory. The instructions are contained in programs that control critical nuclear power plant devices.

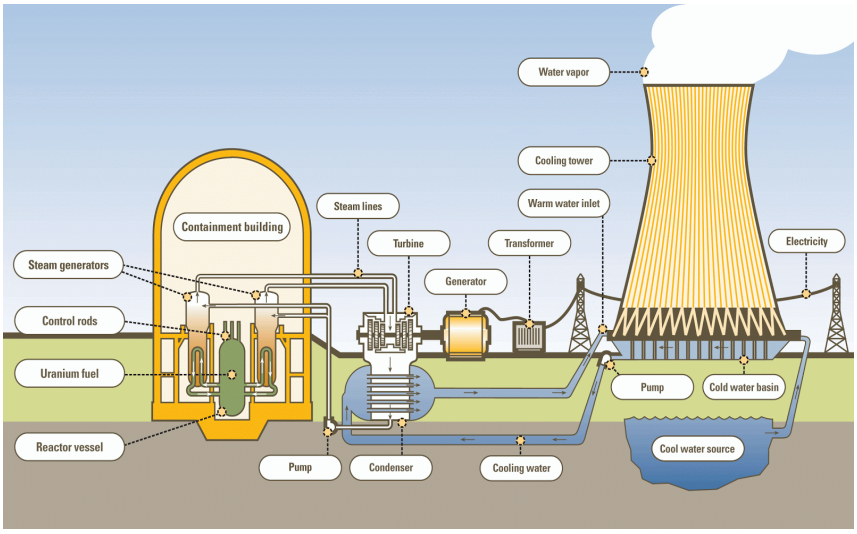


Figure 2 – Nuclear Power Plant[5]

[4] Source: http://map.norsecorp.com/v1
[5] Source: http://www.nuclear-power.net/nuclear-power-plant

New reactors are being designed with an increasing number of digital controls that rely on computers. Nuclear power plant operating and technical support staff use the computers and networks to manage/calibrate the process control systems and other critical infrastructure. These computers play a vital role in monitoring and controlling the operation of the reactors.

Even though a nuclear reactor computing environment can be air-gapped (an air gap is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks),[6] air gaps do not guarantee isolation from the Internet. Office systems at plants often rely on virtual private networks for Internet connections. These networks could be used to tunnel into control systems. Other risks include infrastructure components that are easily identified via a Google search, flash drives that can bridge air gaps and nuclear plant employees who are unfamiliar with key cybersecurity procedures.

If a nuclear power plants radioactive inventory were released in the event of a serious cyber-attack, hundreds of thousands of people could die immediately. Given the potential for great harm, any successful cyber-attack on a nuclear facility would undermine confidence in the ability of the State to host the facility and the owner to run the facility in a safe and secure manner.

New Jersey Nuclear Power Plants

There are three nuclear power plant facilities in New Jersey: Hope Creek, Oyster Creek, and Salem. Hope Creek and Salem are owned and operated by PSEG Nuclear LLC, while Oyster Creek is owned and operated by Exelon Generation Company, LLC. The following is information about these nuclear power plants, including the MWt, which refers to the thermal power produced at the power plant.

| NJ Nuclear Power Plant | Location | Reactor Type | Reactor Vendor | Renewed License | License Expires | Licensed MWt |
|---|---|---|---|---|---|---|
| Hope Creek | Hancocks Bridge | Boiling Water | General Electric | 7/20/2011 | 4/11/2046 | 3,840 |
| Oyster Creek | Forked River | Boiling Water | General Electric | 6/03/2009 | 4/09/2029 | 1,930 |
| Salem | Hancocks Bridge | Pressurized Water | Westinghouse | 6/03/2011 | 4/18/2040 | 3,459 |

[6] https://en.wikipedia.org/wiki/Air_gap_(networking)


Figure 3 – New Jersey Nuclear Power Plants[7]

Nuclear power plants in New Jersey supply approximately 52 percent of the power in the state. A typical plant like Oyster Creek produces power approximately 90 percent of the time, in response to demand for electricity. By contrast, a coal plant supplies power on average 70 percent of the time and a combined-cycle natural gas plant, 60 percent. Solar and wind power, which are subject to variable weather conditions, can be counted on to produce electricity no more than 20 percent of the time. [8]

If a reliable nuclear plant that delivers base-load electricity is taken out of commercial service, the state of New Jersey will have a problem.

## The Stuxnet Worm

In 2010, a malicious computer program (worm) called 'Stuxnet' was manually uploaded into a nuclear plant in Iran. The Stuxnet attack against the Iranian nuclear plant demonstrates the impact that a cyber-attack with a detailed knowledge of process control systems can have on critical infrastructure. Stuxnet took control of and destroyed 984 centrifuges at Iran's uranium enrichment facility in Natanz.

Stuxnet is believed to be a jointly built American-Israeli cyber weapon. Although neither state has confirmed this openly, anonymous US officials have claimed the worm was developed to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents. Stuxnet specifically targeted Programmable Logic Controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery on manufacturing assembly lines and centrifuges for separating nuclear material.

[7] Source:http://www.youdontknowjersey.com/2011/03/nuclear-reactors-in-new-jersey/#!prettyPhoto
[8] http://www.nj.com/opinion/index.ssf/2014/02/opinion_nuclear_power_plans_maintain_a_stable_power_grid.html

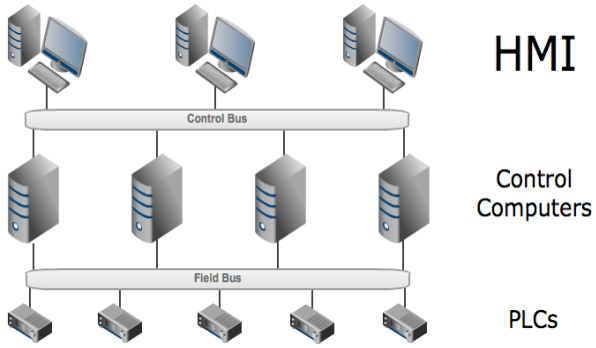


Figure 4 - Human Machine Interfaces (HMI) and Programmable Logic Controllers (PLCs) [9]

Stuxnet targeted machines using the Microsoft Windows operating system and networks, then attached itself to Siemens Step7 Software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.

Stuxnet is typically introduced to the target environment via an infected USB Flash Drive. The worm then propagates across the network, scanning for Siemens Step7 Software on computers controlling the PLCs. Stuxnet introduces the infected rootkit (worm) onto the PLC and Step7 Software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operation system values as feedback to the operator. [10] The Stuxnet worm clearly demonstrates that cyber-attacks cannot be contained; that they can dangerously spread based on their payload, and can potentially create many hazards for critical infrastructure in the nuclear field.

Nuclear Regulatory Commission

The Nuclear Regulatory Commission (NRC) oversees the operation of 100 commercial nuclear power reactors that generate electricity in the United States. All three nuclear power plants in New Jersey are licensed by the NRC. The NRC regulates nuclear power plants through a combination of regulatory requirements; licensing; safety oversight, including inspection, assessment of performance and enforcement; operational experience evaluation; and regulatory support activities.

The NRC has a cyber security team that includes technology and threat assessment personnel who team with other federal agencies and the nuclear industry to evaluate and help resolve issues that could affect digital systems. This team makes recommendations to other offices within the NRC and is also designing a cyber security inspection program for future implementation. The inspection program can

[9] Source: The Vulnerability of Nuclear Facilities to Cyber Attack by Brent Kesler, Strategic Insights, Volume 10, Issue 1, Spring 2011
[10] http://www.computersecurity.org/hacked-website-rankings-ddos-rankings-ratings/stuxnet-apt-plc-attack-rank-this-hack/

serve as an independent and objective audit for the nuclear power plants and include recommendations for nuclear power plant cyber security.

According to the NRC, all power reactor facilities licensed by them must have a Cyber Security Program (CSP) and the NRC requires all critical safety and emergency control systems to be physically isolated from the internet. In the most recent renewal licenses, for each of the New Jersey nuclear power plants, which are approximately 1,600 pages each, there was no reference to the requirement of the CSP. In reviewing the NRC web site, specific to the individual nuclear power plants in New Jersey, there was also no reference to cyber security. Details on plant information, including reactor diagrams, plant videos, inspection reports, and plant operating licensees are referenced and available for review. NRC information/requirements in the cyber security area pertaining to nuclear power plants do not appear to be emphasized in the renewal reports and web site. In addition, the researcher did not come across any information pertaining to NRC cyber-attack threat vector monitoring/analysis or a Computer Emergency Response Team (CERT).

Because of the severe consequences of a cyber-attack on a nuclear power plant, cyber security should become more of an emphasis.

**What are the Vulnerabilities?**

The extent to which a nuclear power plant is vulnerable to a cyber-attack will depend upon the design of the plant, the technical and organizational history of the plant, how and which computers are used, whether the computers allow for internal and/or external networked interactions, and how effective the countermeasures employed are at preventing attacks or mitigating the consequences of any attacks that succeed. [11]

There are a number of types of cyber-attacks that could affect the operation of a nuclear power plant. These cyber-attacks are evolving as well. These cyber-attacks include:

- Infection via known connections to the Internet.

  Nuclear facilities that allow third-party remote access may open up several avenues by which hackers can gain access. Owner/operators could possibly create direct links between their business networks and facilities and industrial control systems. The owner/operator's commercial network can serve as a route of infection.

- Virtual Private Networks (VPN) providing a route for a cyber-attack.

  Plants permit vendors to access facilities remotely through a VPN connection, which allows individuals to connect to a private network over the Internet via a secure encrypted circuit. If the VPN is insecure, it can be a source of vulnerability, making it possible for malware to find its way onto the industrial control network.

[11] http://www.state.gov/t/isn/183589.htm

- Infection via undocumented connections to the Internet.

  Nuclear power plants could have undocumented connections to the internet (i.e. connections of which the plant managers or owner/operators are unaware). These connections can provide a potential pathway to gain access to the internal network.

- Contractors or employees set-up rogue or unauthorized connections.

  Even though wireless connections are generally strictly forbidden at nuclear facilities, a contractor might**,** for reasons of convenience, install a wireless network in the office without informing systems administrators.

- Contractors or employees inadvertently installing equipment that has Internet connectivity**.**

  When a part wears out in a facility, a contractor might replace it with a new part that could have exactly the same serial number as the old part, leading the contractor to believe that it is exactly the same. Yet the vendor might have added a Wi-Fi or GPS functionality that provides a mode of access for a hacker.

- Use of "war dialers".

  A hacker could find modems connected to the programmable circuit breakers of the electric power control system by using a personal computer program that dials consecutive phone numbers looking for a modem. The hacker could crack the password that controls access to the circuit breakers, and change the control settings to cause power outages in the plant that could result in damaged equipment.

- Infection despite being air gapped.

  Even when nuclear facilities are air gapped, there are still a number of possible routes of infection. While an air gap does reduce a facility's vulnerability, it does not provide complete protection. For example, in the Stuxnet cyber-attack, malware can infect the nuclear facility when a USB drive or other removable media device is plugged into the plant network.

- Misunderstanding connectivity.

  Despite the use of the air gap within nuclear facilities, a number of nuclear plant personnel and even owner/operators of facilities may not necessarily realize that their nuclear facilities have Internet connectivity, or fully understand its implications.

**Recommendations**

To emphasize the importance of cyber security and further protect the nuclear power plants, the State of New Jersey should consider establishing a Cyber Security Center for nuclear power plants and share information vis-a-vis the nuclear power plants in New Jersey.

In conjunction with the Nuclear Regulatory Commission, the New Jersey State Cyber Security Center could assist in overseeing the nuclear power plants cyber security plans, monitor cyber-attack threat vectors, perform the roles of a CERT, and work with the nuclear power plants to:

- encourage them to share intelligence on evolving threats and information associated with the source of an attack
- identify and define the specific employee skills required to protect against nuclear cyber-attacks
- identify education and training organizations/institutes with expertise in cyber security and encourage attendance/participation
- encourage the implementation of "best practices" in cyber security
- identify computer hardware and software intended to be immune to cyber-attacks
- identify mechanisms for detecting the source of cyber-attacks
- establish communication strategies and associated security protocols to facilitate information sharing and problem solving

The New Jersey nuclear power plants, in conjunction with the State of New Jersey Cyber Security Center can design robust security architecture for their plants and work together to implement cyber security mechanisms at the level of each reactor. They could implement security architecture and systems aimed at reducing potential vulnerabilities and preventing cyber-attacks. Such a security architecture and associated cyber security mechanisms could include:

- preparing a detailed information technology diagram of the nuclear power facility that includes the locations of any potential vulnerabilities
- conducting a risk assessment on an annual basis, identifying any new cyber-attack threat vectors, there probability of occurrence, and impact
- establishing security policies, standards, and procedures, which include minimum security baselines
- implementing intrusion detection capabilities for detecting abnormal instructions
- implementing capabilities for detecting attempts to gain unauthorized access
- limiting network access, preferably disconnecting all critical areas from networks

## Conclusion

While nuclear power plant facility operators are rigorous about enforcing rules that pertain to physical safety and security, they may be less rigorous when it comes to rules that concern cyber security. To be successful in combating the cyber threat in New Jersey nuclear power plants, the power plant owners/operators in conjunction with the proposed State of New Jersey Cyber Security Center should

work together to design a comprehensive security architecture for the plants; establish computer emergency response protocols; and implement cyber security mechanisms at the level of each reactor. This collaborative approach, when combined with the use of technology, can help ensure that cyber-attacks are both prevented and deterred.