Short Article ISSN 2767-3901

International Journal of Theoretical & Computational Physics

Cost-Effectively Detecting, Preventing and Mitigating Cyber Threats to Nuclear Energy Systems

Bahman Zohuri[1*], Akansha Agarwal Dinesh Kumar[1] and Masoud Moghaddam[2]

[1]*Golden Gate University, Ageno School of Business, San Francisco, California 94105*

[1]*Galaxy Advanced Engineering, Chief Executive Officer*

[2]*AICyberDomain.com, Chief Executive Officer*

***Correspondence author**

Bahman Zohuri
Galaxy Advanced Engineering,
Chief Executive Officer
New Mexico

Submitted : 9 Mar 2022 ; Published : 24 Mar 2022

Citation: Zohuri B.,Dinesh Kumar A. A., Moghaddam M., Cost-Effectively Detecting, Preventing and Mitigating Cyber Threats to Nuclear Energy Systems. I J T C Physcics, 2022; 3(1): 1-3.

Abstract

Cost-effectively detecting, preventing, and mitigating cyber threats are a concern for most organizations, especially those in critical infrastructure sectors. The electrical and mechanical equipment for nuclear power plants is very important to nuclear safety and dependent upon computer-based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. Security systems do not need more tools, they just need more rules, because fighting new threats with more tools just adds complexity and more degrees of freedom; that these new tools always bring on board. It is time to rethink our approach to Cyber Security.

Keywords: Resilience System, Energy Flow, Energy Storage, Energy Grid Business Intelligence, Artificial Intelligence, Cyber Security, Decision Making in Real-Time, Machine Learning, and Deep Learning, Big Data and Cloud-based servers for repository and storage of Data.

Introduction

Developing an integrated and intelligent approach to securing your information technology environment was and has always been a concern of most organizations in past few decades. Security Intelligence, Data-Driven Analytics, Proven Expertise, Real-Time Defenses, Types: Incident Response, Endpoint Management, Threat Intelligence, Network Security, Fraud Protection. With demand for energy and an essential element of our day-to-day operation energy in form of electricity has tremendous impact and effect in our life, thus the security of such source of necessity is very important to us and owners of such resource production and their facilities when it comes to the operation of their power plant and control room that is part of the Internet of Things and net of Machine-to-Machine integration. Grids of electricity and network augmented to each other in order to support the demand for electricity every day either in peak or off-peak, thus Cybersecurity plays a big role in the protection of such assets at our disposal. Early detection will help in cost-effectively mitigating these risks. With help from Artificial Intelligence (Zohuri & Mossavar Rahmani, 2019; Zohuri & Zadeh, 2020) integrated into the Internet of Things, we can build a resilience system that will protect our grid system nationwide and will be able to predict any malicious attack in form of energy blocks Malware before it attacks (Zohuri, et al., 2022; Zohuri & Moghaddam, 2017).

"What makes cyber threats so dangerous is that they often go unnoticed for a while, until the real damage is done, from stolen data over power outages to destruction of physical assets and great financial loss. Over the coming years, we expect cyber risks to increase further and change the way we think about integrated infrastructure and supply chain management."

It is impossible to overstate the importance of energy. Just thinking where humanity would be without it may be enough to demonstrate this point. Like in the past, energy will play a vital role in shaping future industries, cities, nations, and the world. With the growth in population at 18% globally, demand for electricity and consequently the source of energy to produce its electricity is on the rise also, thus securing such valuable source of generating electricity via renewable or nonrenewable methods in a cost-effective way is vital as well.

As we know, with technology Nuclear Power Plants (NPPs) at least from fission processing point of view moving from third generation (GEN-3) to the fourth generation known as (GEN-IV) using Small Modular Reactor (SMR) technology progressively perused by engineers and scientists in the recent past decade and continue growing as a means of producing energy as a source of electricity generation (Zohuri &

McDaniel, 2019; Zohuri, 2018).

The possible structure of Nuclear Power Plants (NPPs) network computer systems can be divided into two separate types:

Internet: The Internet is a global system of interconnected computer networks that use the standard Internet Protocol (IP) suite to serve billions of users worldwide. Representing the homepage of NPPs must be connected to the internet so that people can access the homepage to get general information about NPP.

There are also some other information systems that are publicly open for the purpose of taking applications from job-seekers or contractors in case of new work or supply chain perspective as well.

Internet-directed threats in NPPs are mostly mitigated by network architecture and data diodes. Threats from the supply chain, portable media, and insiders are more of a concern.

Intranet: An internet is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or network operating system within that organization. Actually, there are two types of internet:

- The private network is connected to the Internet, but it is protected by information security systems such as Firewall or Intrusion Protection Systems (IPS).
- The private network is physically isolated from the outside network.

It is important to classify the functions, systems, and equipment of Nuclear Power Plants (NPPs) into safety classes. The purpose of the classification is to guarantee that each object in the NPP is getting the required attention based on its importunate to safety. With demand for energy as an essential element of our day-to-day operations, energy in the form of electricity has a tremendous impact on our lives. The security of this source of energy is very important to our economy and society. The owners of the energy generation such as utility companies, and distribution facilities are very conscious of their vulnerabilities due to Machine-to-Machine integration and cyber-physical inter-relationships.

The interconnection of networks in NPPs can be composed of seven components:

1. The Emergency Response Facility (ERF) system,
2. The Engineering Safety Feature (ESF) system,
3. The Plant Control Systems (PCS),
4. The Physical Security Protection (PSP) system,
5. The Reactor Protection System (RPS),
6. The Radwaste Treatment System (RTS), and
7. Turbine Control System (TCS).

Among the control networks, we concentrate on the ERF system and the PSP system, which are the only routes to provide information outside thus cyber security as well as physical security are critical issues in analyzing control systems in NPPs.

Building such infrastructure and resilience system in places, where these nuclear power plants are operating is not going to be cheap and requires a means of cost-effectiveness analysis from both Total Cost of Ownership (TOS) and Return on Investment (ROI) perspective and utility owners can comfortably invest in it accordingly.

NPPs use multiple Instrumentation and Control (I&C) systems that may be interconnected in various ways, including I&C for reactor safety, namely the reactor protection system, reactor control, plant control, and plant health monitoring. The design of I&C for Reactor Protection depends strongly on the physical design of reactor safety systems. Existing nuclear plants generally use "active" safety systems with multiple, active pumps, valves, and electrical power supplies capable of performing heat removal under normal shutdown and accident conditions. New "passive" designs for advanced nuclear reactors can perform these shutdown heat removal functions without external sources of power or control and are activated to perform these functions by disconnecting external sources of power and control. However, they still require I&C to sense conditions.

The possible threats of the control networks in Nuclear Power Plants (NPPS) can be identified as:

- NPP Instrumentation and Control (I&C) systems generally use closed data and communication networks or air-gasp such that access through the Internet to the systems becomes difficult.
- However, recent cases of Advanced Persistent Threat (APT) or Modern Malware attacks demonstrate that NPP I&C systems may also be infected by malware enabling cyber-attacks through portable devices such as notebooks, Personal Digital Assistant (PDA), and USB thumb drivers.
- It is very important to identify all the connection points between humans with external electronic devices and the I&C systems and to analyze potential security breaches that can be exploited by cyber threats. These connection points are usually related to plant maintenance and test tasks.

This research and Technical Memorandum (TM) focus primarily on NPP I&C for reactor safety functions. It reviews current best practices for digital control of existing plants that use active safety systems. The key question that emerges is how cyber security best practices for existing nuclear reactors with active safety systems are relevant to advance passive nuclear reactor control systems.

Cyber security: plays a big role in the integrity and protection of such networks and assets. Artificial Intelligence integrated with the Cyber-Physical Systems (CPS) can build a resilience system that will protect. It will enable us to identify any malicious attack in the form of malware before the attack

begins. However, as the malware attacks are evolving, the security systems should also cope with them.

Security systems do not need more tools, they just need more rules, because fighting new threats with more tools just adds complexity and more degrees of freedom, that these new tools always bring on board. It is time to rethink our approach to cybersecurity.

With all the above privileges utilizing Internet of Things (IoT) and Artificial Intelligence (AI) as combined innovative technology of Device-to-Machine (D2M) and Machine-to-Machine (M2M), they harness the sensor data to boost uptime, performance, and productivity while lowering maintenance costs and reducing the risk of revenue loss.

Major Deliverables and Outcomes

If any utility and energy-producing companies that own any Nuclear Power Plants of fission type, would like to invest in such system a resilience system as suggested above, based on these authors' investigation and research a holistic project plan along with dollar amounts can be taken into consideration as follows:

Year 1

Reviewing the structure of the NPP Connectivity and Vulnerabilities in terms of Device Connectivity, Human Connectivity, Contractors Involvement, and Network Access Levels and creating a Comprehensive Approach to address current and evolving threats to our grid in order to provide a total solution to eliminate current and future threats.

Year 2

A report detailing a software algorithm system design for the purpose of Cyber Security using Artificial Intelligence in the form of a Control Panel Demo based on Python or C++ language.

Year 3

Proposing a Fully functional AI-Assisted software package based on DL/ML [2] to be used in some test facilities with proposing security methods to have more control over human involvement and interaction within their access levels to power grids control systems and any modifications

All three steps above are the most cost-effective approach to Detecting, Preventing, and Mitigating Cyber Threats to Nuclear Energy Systems as it has been laid out in this technical memorandum here.

Conclusions

We as the authors believe that from ownership and cost-effectiveness of such a resilience system in place for any operational NPPs, given the thrive of Internet-of-Things (IoT) technology, there exists no other alternative solution around and against modern and smart malware due to cyber-attack and cyber-warfare that these owners are facing. Investment in such a system in a long run is the most cost-effective of protecting your Nuclear Power Plants that are now getting to be in demand based on supply chain and supply and demand of energy driven by population growth around the world.

References

1. Zohuri, B. & Mossavar Rahmani, F. (2019). Artificial Intelligence Driven Resiliency with Machine Learning and Deep Learning Components", Short Article, *International Journal of Nanotechnology & Nanomedicine, 4*(2), 1-8.
2. Zohuri, B. & Zadeh, S. (2020)."Artificial Intelligence Driven by Machine Learning and Deep Learning", First Edition, *Nova Science Pub Inc*, DOI: 10.52305/LFWK9582
3. Zohuri, B., Moghaddam, M., & Mossavar-Rahmani, F. (2022). "Business Resilience System Integrated Artificial Intelligence System", *International Journal of Theoretical & Computation Physics,* February 2022 issue being published.
4. Zohuri, B. & Moghaddam, M.(2017). "Business Resilience System (BRS): Driven Through Boolean, Fuzzy Logics and Cloud Computation: Real and Near Real Time Analysis and Decision Making System", 1st Edition March 17, 2017, *Springer Publishing Company.*
5. Zohuri, B. & McDaniel Patrick. (2019)."Advanced Smaller Modular Reactors: An Innovative Approach to Nuclear Power", *Springer Publishing Company*; second edition. 2019 edition. Electronic ISBN: 978-3-030-23682-3
6. Zohuri, B. (2018). "Small Modular Reactors as Renewable Energy Sources", Springer Publishing Company; 1st ed. 2019 edition, 1–61, DOI:10.1007/978-3-319-92594-3_1