CONSEQUENCES OF CYBER-ATTACKS IN A NUCLEAR SECURITY SYSTEM OF A BRAZILIAN NUCLEAR POWER PLANT

Fiel, João Claudio Batista

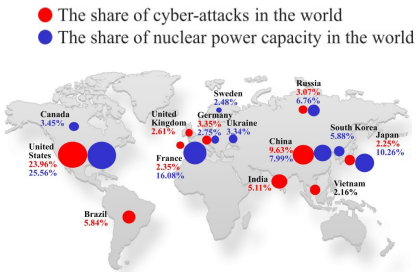
Nuclear Engineering Department, Instituto Militar de Engenharia, Urca, Rio de Janeiro, Brazil.
fiel@ime.eb.br

1. Background and Goal of the present work

Today, there has been a growing increase in increasingly complex cyber attacks targeting a variety of information, telecommunications and control (I&C) systems, including nuclear plant and facility systems. Many of these attacks primarily target the safety and control systems of these nuclear power plants, as well as the various subsystems of the instrumental and control systems, such as engineering workstations, physical security systems, reactor protection systems, among others. others. In defense of power plants and nuclear facilities, in response to the growing threats from cyberspace, investment in computer simulations, regulations and technologies to protect and enhance the cybersecurity of I&C systems has increased in Brazil.

Due to the rise in cyber attacks worldwide, various regulations and standards have been made in Brazil to increase the prevention and mitigation of cyber threats. In parallel, an increasing number of research is being conducted focusing on the assessment and protection of Brazilian cyber security. As a demonstration of the various studies conducted to implement improvements in cyber defense systems, a cyber security work has recently been developed describing an assessment of the impacts of cyber attacks on the security system effectiveness of a hypothetical Brazilian facility comprising a small modular reactor. type iPWR. Performance data was extracted from various sources in the IAEA. The methodology uses a performance-based approach to calculate the probability of effectiveness (PE) of the baseline system, as well as the decrease of PE under the interference of cyber threats.

Understanding what are the main cyber attacks, how they are implemented, what their consequences are, how to analyze, evaluate and predict cyber threats as well as what protection mechanisms, and what are the ideal ways to deploy them, are beneficial to researchers and professionals. Figure show Collocation of World Major Cyber-attacks Source and Nuclear Energy cappacities



In the simulation cited, some attack scenarios are postulated to assess the influence of this threat on a security project. Postulated scenarios include credible cyber attacks on computer systems that control external, internal, position, and seal sensors. Under these simple scenarios, an outsider's likelihood of interruption (PI) would decrease to low levels. Consequently, in most scenarios, even with full probability of neutralization (PN), it would not be possible to mitigate the threat in a timely manner, making it possible to perform a mixed attack. From the results obtained in this work, it is possible to easily identify the level of security that should be associated with nuclear installation cyber systems as indicated by the NSS-17G.

2. General View about Ciber Attacks

Nowadays it is known that with the predominant installation of information and communication devices in nuclear facilities, synthetic engineering systems have undergone a transformation from conventional physical systems to more complex cyber-physical systems. We can observe over the years, a worldwide increase of cibe attacks, applied to different information systems, telecommunications and control (ITC). In Brazil, there is currently a growing concern about the rise of cyber attacks in the world, especially with the use of malware by hackers, which could access domain control accounts and hack critical plant systems. As a result, the government has increased its investment in technology resources for nuclear cyber defense.

Although the critical systems of Brazilian plants and facilities have never been affected by this type of attack, there is concern and consequent prevention against this possible threat, where malware used to rob ATMs could invade the administration of a nuclear plant. Hackers may not be able to manipulate control systems, but may use malware to steal information or infect other devices on the network.

In general, opponents with cyber capabilities can perform attacks in four broad areas: Attack on systems linked to Physical Protection, Attack on systems linked to Safety Technology, Attack on systems linked to the Control and Accounting of Nuclear Material and, Attack on systems linked to Information Technology (T.I.).

3. 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.

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-ofservice (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.

4. Cyber Security System Design in a Brazilian Nuclear Installation

For the purposes of the analysis of this work, the organization of these systems was postulated as follows.

The first of the cyber systems in this facility is where the magnetic door opening sensors, classified as position sensors (SNL, 2018) are connected. This cyber zone was named in this work as the “position sensor system”. This system is networked to the central and secondary alarm stations.

The second of the RAMPeM complex cyber systems is where the infrared sensors - inside the Protected Area - as well as the vibration and electric field sensors installed on the Protected Area fence are connected.

It is worth noting that the SNL classification (2018) tells us that the vibration and electric field components are classified as elements of the so-called “fence sensors”. Only infrared sensors constitute the elements called “external sensors”.

However, these sensors are located outside the buildings that make up the RAMPeM complex. Thus, this cyber zone has been aggregated all these sensors and is called “external sensor system”. This system - like the position sensor system - is networked to the central and secondary alarm stations.

Finally, the last of the RAMPeM cyber systems is where the Closed Circuit Television (CCTV) cameras are connected. It is noteworthy that the SNL classification (2018) tells us that the video components in an installation can be classified as “internal sensors” or “external sensors”, depending on where these cameras are located.

However, CCTV elements - along with lighting elements - make up the alarm assessment. Therefore, they are an important part of the security of an installation as they will allow to correctly communicate whether the location is under attack or not.

Thus, this cyber zone unifies these sensors and is called “CCTV system”. This system is networked to the central and secondary alarm stations, in addition to the Guard Room - adjoining the control room entrance, as shown in the figure.

5. Conclusion

Understanding what cyber attacks are, how they are implemented, what their consequences are, how to analyze, evaluate and even predict how cyber threats, what protection mechanisms, and how to optimally implement them, are beneficial to both. . researchers and professionals. In this article, we present an overview of the above aspects related to NPP cybersecurity in recent years. The results of this review show some potential approaches for future research’. Using the approach allows us to identify vulnerabilities of the model itself - in this case, or DEPO process - given as requirements of each of the Nuclear safety areas. From the results obtained, it became evident that the adoption of a methodology applied in performance represents a significant evolution in the evaluation of physical protection systems.

However, adoption is not enough if it is not synergistically integrated into cyber security. Because simple simulations of cyber attacks on the benchmarking system have led to a likelihood of disruption of the adversary - and in some cases of global system threats - the use of SisPF vulnerable to internal and external testing.

However, the results obtained allow us to infer that the use of the performance approach - DEPO process form - has potential use as the (initial) detection tool of which cyber systems are most vulnerable and, therefore, may compromise integrity of a nuclear facility when under attack - whether internal or external adversary.