A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Security Audit and Assessment Literature Review

Thomas MacKinnon TP066728
Intake Code: APDMF2204CYS(PR)
Module Code: CT114-3-M-SAA
Yogeswaran A/L Nathan
Date Assigned: 05/10/2022
Date Completed: 18/11/2022
Word Count: 2495

Abstract

The Corona Virus has seen to a massive rise in Cybercrime, effecting every industry greatly, with more successful attacks everyday. This is particularly concerning when it comes to critical areas of industry, like Nuclear facilities, which provide power throughout the nation, making it a prime target to malicious actors. The power to not only leave large areas of the country in the dark but also the dangerous materials found in Nuclear Facilities makes it even more appealing, as the potential damage from a successful attack could be disastrous.

This paper aims to research the state of nuclear facilities, and discuss some of the key threats faced in the past. The recommendation of authors and from international standards leads to the conclusion that security auditing is the key way at ensuring security and safety at facilities, which will be covered in the next report.

Contents

List of Figures

1 Introduction

Nuclear Facilities have been a staple of energy provision from the 1950s, still being a critical area of a countries power generating capabilities. Nuclear Facilities by there very nature are dangerous environments if left in the wrong hands, and can have catastrophic consequences if attacked by a Malicious actor. Radiological damage can leave vast areas of land uninhabitable for generations, nuclear meltdowns can kill thousands, and even destabilise governments. The rise in Cybercrime only adds to the worries surrounding Nuclear Facilities, as it opens a new level of entry points for Malicious actors to attack from. Cybercrime has seen a great rise over the last ten years, as seen by Figure 1, which is a worrying statistic to Nuclear Facilities wishing to remain safe and secure. This raises the question of what threats exist towards Nuclear facilities in 2022? and what preventive measures can be put in place to mitigate the risk of Cybercrime?

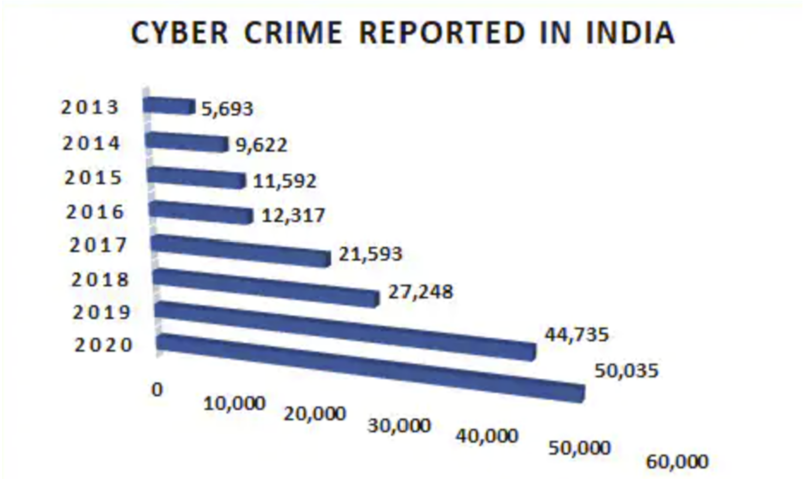


Figure 1: Rise in Cybercrime in India, from 2013 to 2020 (Singh, 2021)

This report is in two parts, the first section will Review Literature related to Nuclear Facilities, assessing how they operate at the time of writing, what security threats they have faced, and what standards they have to comply with. The aim of this is to find any areas where research is lacking, which will then be developed and expanded on for the second part of this report.

2 Literature Review

This Literature review aims to give an overview of how Nuclear Facilities operate in the modern age, by sourcing information from Academic Literature retrieved from reputable sources, such as the Association for Computer Machinery (ACM) or the Institute of Electrical and Electronics Engineers (IEEE). The Review consists of four sections of research to give a full understanding of Nuclear facility security whilst trying to uncover areas where research is lacking.

2.1 Nuclear Facilities in the modern age

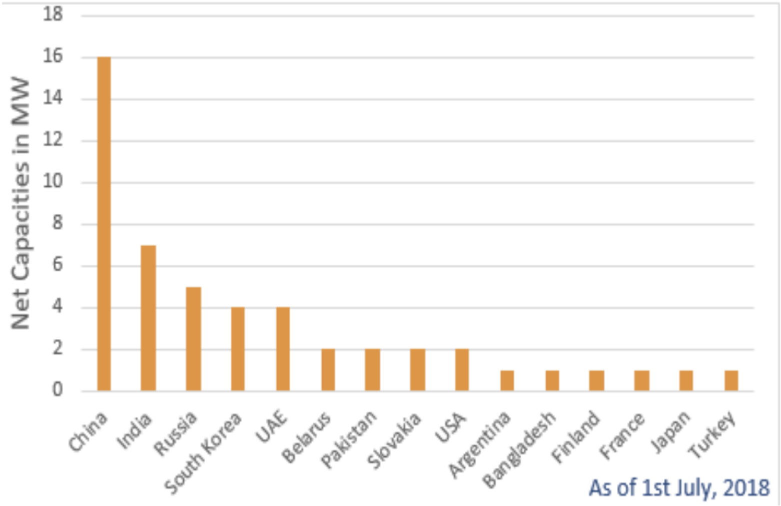


Figure 2: Construction of Nuclear Reactors under Construction in various Countries (Akinlabi et al. 2018)

Nuclear Facilities have been used to supply countries with power for over fifty years, the first being the Obninsk Plant in the Soviet Union, which began operating in 1954. However, since then the state of Nuclear enegy has greatly changed, which is detailed by Akinlabi et al. (2019) in [3]. The researchers convey that Nuclear energy since its discovery has always been dangerous, aiming to give solutions to incorporating the proper safety and security into facilities. The authors state that the push for Nuclear security came after the meltdown of the Chernobyl power plant, which shocked the world with how dangerous Nuclear facilities could be if the correct procedures are not being followed. The Chernobyl disaster not only irradiated a large area of land, but is also credited as aiding in the dissolution of the Soviet Union, truly the effects of mismanaged Nuclear Facilities are greater than any other Industries. The researcher further state that reactor meltdowns are not a thing of the past, referencing the Fukushima disaster, and stating that the threat of terrorism is very concerning, as Nuclear sabotage could be catastrophic. Chernobyl was caused by irresponsible testing, so it is a fair enough example to bring up in the paper, however, Fukushima was caused by a large scale earthquake, which is less applicable. Still, if the Japanese Atomic Energy Agency had specified backup power generators in Facility design the disaster could have be averted, leading to many saved lives. As more and more Nuclear Facilities are being constructed the proper safety and security procedures need to be put in place to avoid potential disasters. Nuclear Energy is a growing industry, with many plants under construction, as seen in Figure 2, which does raise the concern that speedy development is better prioritised over facility safety. Overall the paper by Akinlabi et al. (2019) in [3] is excellent, giving a concise history on the field of Nuclear power with interesting examples, and provides research that will be used throughout the rest of this Literature review.

The rise of the internet has led to increasing need for security for Nuclear Facilities, as Cyber threats have become a serious concern to all industries. Cyber threats have been classified on the same level as international terrorism and serious national disasters under the United Kingdom's Security Concern list (Litherland et al. 2016 in [8]). The Corona Virus Pandemic was only increased the risk from Cyber threats, according to statistics derived from the Federal Bureau of Investigation's Internet Crime report (FBI, 2020), which is conferred with further reports stating that Cybercrime has risen over 600% in recent years (Purple Sec, 2022).

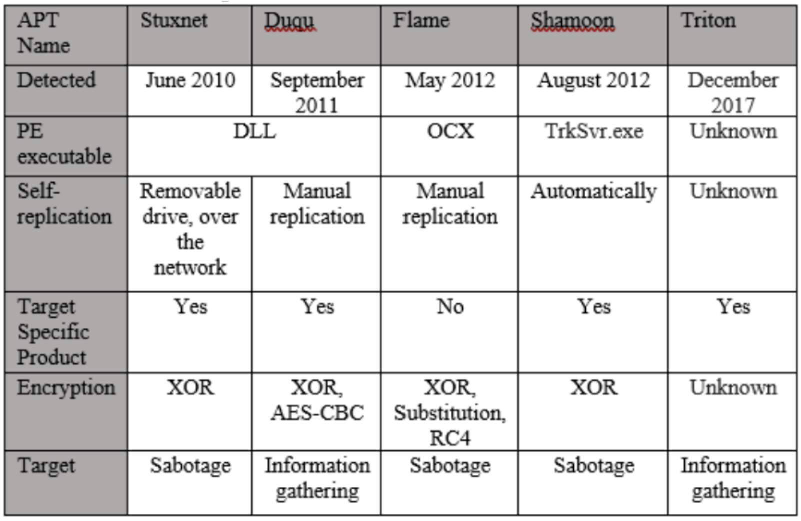
Ahuja et al. (2020) in [1] state that this is due to people being online more than ever as a result of self quarantining measures. Their paper relates to the possible Cyber threats that working from home presents to employees and the organisation as a whole, as many businesses required staff to continue working whilst off site. Insecure connections, malware, and rogue WiFi broadcasts were all discussed in the paper, highlighting how these vulnerabilities would normally be mitigated by an organisations firewall or security mechanisms, but are left unchecked by Work from home mandates. Nuclear facilities were exempt from staff quarantining, as they are regarded as an essential industry, but remote access technology still exists within power plants. This paper was reviewed to give an idea of how Facilities are effected during Covid-19, and what potential vulnerabilities remote access Facility systems could give to malicious Hackers. The paper presents a good method for staff to secure their devices to protect the organisations network, but is not as applicable to the subject at hand.

The final paper reviewed for the state of Nuclear Facilities in the modern was by Hellman (2017) in [5], which discussed a variety of topics. The researcher states that the threat to Nuclear Facilities is greater than ever, and that Cyber warfare is likely to target these critical industries , so the proper security and safety needs to be put in place to mitigate disasters from happening. Hellman also highlights the that Nuclear weapons are often used as a deterrent to prevent attacks against themselves, as mutually assured destruction aids no one. The author states that Cyber weapons could become a new deterrent, acting as way to prevent other opposing Governments or political bodies from launching Cyber attacks against critical industries like Nuclear Facilities in fear of the possible retaliation. Overall the paper gives some interesting ideas about the state of Nuclear security and how vital a proper defense is to continuing safety, but is rather disjointed. The author covers several topics but does not properly link them together, making the paper feel more like a series of thoughts rather than a cohesive statement. Furthermore, the paper fails to bring up any key threats faced by Nuclear Facilities, leaving the reader unclear to the danger that is out there.

2.2 Threats to Nuclear Facilities

Nuclear Facilities are a prize target to any Malicious actors wishing to cause damage, either in monetary losses, reputation (of facilities or political parties), data loss, to even extremes of loss of life, destruction of property, and ecological damages.

Stuxnet is a very well known computer worm that targeted Iranian Nuclear facilities around 2010, destroying an estimated nine hundred uranium enriching centrifuges, and is thought to be the first virus capable of crippling hardware. Madnick & Nourian (2018) in [9] detail how stuxnet so effectively dismantled the security in place at the effected Nuclear facilities. Stuxnet exploited a piece of software named *Siemen's step 7*, which allowed control of the Programmable Logic Controllers (PLC) associated with enrichment centrifuges. The worm would send damaging commands to PLCs whilst reporting normal readings to staff, so as the machinery is being destroyed staff are left in the dark. Iran's Nuclear Facilities are not connected to the internet to mitigate potential Cyber attacks, so Stuxnet spread through the use of USBs taking in by employees, showing that even air tight security in Nuclear Facilities allow for breathing room. The researchers describe how the worm would spread using Windows Autorun, and infected roughly 200,000 machines. The paper is incredibly interesting, and shows the damage that a gap in security can cause to Nuclear Facilities. The remainder of the paper focuses on preventing Stuxnet at the design level, so was out of scope for this project, but still enlightening nevertheless.



APT Name	Stuxnet	Duqu	Flame	Shamoon	Triton
Detected	June 2010	September 2011	May 2012	August 2012	December 2017
PE executable	DLL		OCX	TrkSvr.exe	Unknown
Self-replication	Removable drive, over the network	Manual replication	Manual replication	Automatically	Unknown
Target Specific Product	Yes	Yes	No	Yes	Yes
Encryption	XOR	XOR, AES-CBC	XOR, Substitution, RC4	XOR	Unknown
Target	Sabotage	Information gathering	Sabotage	Sabotage	Information gathering

Figure 3: Sons of Stuxnet characteristics (Al-Rabiaah, S. 2018)

Stuxnet was not the only Cyber attack to target power generating stations like Nuclear Facilities, as Greenberg's novel (2019) in [4] on the subject describes. The malicious Cyber weapon named "Black Energy" was launched against the Ukrainian electricity grid in December of 2015, and later again a year later (this time named "Indostroyer"). The author refers to these as the "Sandworm Attacks", which like Stuxnet targeted industrial control systems, and caused major power outages throughout the city of Kyiv and regions of the country. The hacking group responsible was based in Russia, and heavily suspected to be funded by the government, who had recently annexed Crimea. It can be argued that these attacks were Russian trials before the invasion of Ukraine, the power to shut off an entire countries power would greatly aid any attacking force. The author suggests that the Sandworm attacks are only the first of a new generation of Cyber threats towards critical industries, highlighting that Nuclear Facilities in particular are a key target to any opposing force. The novel is incredibly interesting and well written, but lacks technical depth into the attacks, focusing far more on the story of discovering the Sandworm hacking group. The authors predictions of the future are haunting to say the least, and show very effectively the real threats Nuclear Facilities must secure themselves against.

Al-Rabiaah (2018) in [4] agrees with Greenberg's (2019) statements in their paper on Advanced Persistent Threats, where the author states that attacks against Nuclear Facilities are likely to continue. There are several other Cyber attacks like Stuxnet and the creations of Sandworm, which target different aspects of critical infrastructure. Duqu is a notable example as this worm was discovered only a year after Stuxnet, attack similar targets but this time with the aim of gathering information, like emails and passwords through key-logging. Shamoon came a year after that, attacking the oil and energy sectors in the middle east, with an estimated 30,000 destroyed workstations as a result. Triton is the most recent example the author gives, which was discovered in 2017, and targeted industrial control systems in Saudi Arabia. Triton, like Duqu, focused on information gathering, with both worms suspected of being used to find methods for future attacks. The paper is very informative of the nature of attacks against the energy sector, providing many examples of supposed "Sons of Stuxnet", as seen in Figure 3, but lacks solutions to fix these vulnerabilities to prevent danger to more Nuclear Facilities in the future.

2.3 Standards to follow

The threat to Nuclear Facilities is clearly great, which is why it is important for the proper procedures and policies to be in place as to keep this critical industry safe. Several papers researched contained different standards to follow to mitigate the risk of nuclear disaster.

IEEE (2021) in [6] shows the correct security systems that should be put in place at Nuclear Facilities, through physical and digital mediums. The paper highlights that both aspects of security should be taken very seriously as to avoid attacks, and that physical vulnerabilities in security can led to digital attacks (with the opposite being true too) as in the case of Stuxnet. It is interesting to see a document released after an attack adopt the necessary strategies to avoid future threats, showing the lessons learnt from Stuxnet. The paper details various digital threats and the security mechanisms needed to prevent them, such as intrusion detection software and application whitelisting. The paper is a good standard for security, but lacks depth in fields, preferring to give an overview as a whole rather than be as informative as possible. Perhaps this was a choice to make the document more readable to Nuclear Facility staff, so that fixes could be made as soon as possible. The paper also dives into physical security through perimeter alarms, video surveillance, and access controls, but is rather lacking in this field.

The United States Nuclear Regulatory Commission (U.S.NRC, 2013) greatly make up for this lack in the IEEE document, in the official Nuclear Power Plant Assessment guide. The paper focuses on properly auditing a Facilities physical defence and security mechanisms against threats, whether they be malicious insiders or even invasion forces. This paper covers all aspects of physical security, from possible entry points to most efficient route to critical resources, as to understand how an enemy would attack a facility. This information is used to develop countermeasures, such as deployable barriers, automated weapons, and highly trained security teams. The paper makes reference to Cyber attacks, stating they could be done in conjuncture with physical attacks, however, lacks much depth into preventing such an attack. The document is excellent otherwise, and perhaps if used in combination with the IEEE standards that focus on digital threats could create a very effective security solution for Nuclear Facilities.

2.4 The need for Security Auditing

Failure to properly observe and follow Nuclear Facility Standards and regulations could be catastrophic, causing untold damage. Security Auditing is a process of evaluating how an organisation conforms to the aforementioned standards, aiming to uncover any vulnerabilities before an attacker can. Several authors suggested that regular compliance checks should be performed at critical infrastructure like Nuclear Facilities, so Security auditing is the obvious solution. Furthermore, Akinlabi et al. (2019) in [3] state that Nuclear security standards differ from country to country, and even from state to state. The authors present the image seen in Figure 4 about the core ways to improve Nuclear safety, "Transparency and mutual trust" and "Regional Coalition on Safety matters" are both good and effective options, but are out of reach for Nuclear Facility operators.

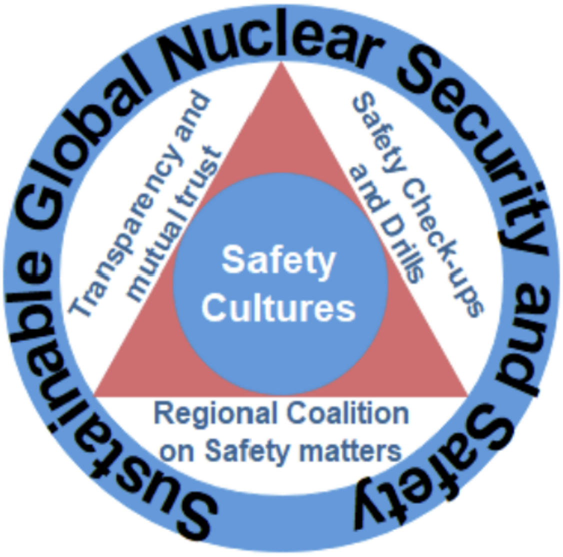

Sustainable Global Nuclear Security and Safety
Transparency and mutual trust
Safety Check-ups and Drills
Safety Cultures
Regional Coalition on Safety matters

Figure 4: The core principles of Nuclear Safety and Security (Akinlabi et al. 2019)

The final core tenant of Nuclear security and safety is "Saftey Check-ups and Drills", which is easily incorporated into an Audit. This research reveals the multitude of threats that face Nuclear facilities, and the troubled history the field has faced. From the papers reviewed it is clear that proper Security auditing through use of a detailed checklist is necessary to securing this critical industry, by combining digital audits with physical checks to ensure total security throughout a Facility. This leads to the second part of this report, which will cover the constructed checklist and how it would hypothetically be used in a Security audit.

3 Conclusion

In Conclusion, the current state of Nuclear Facilities in the modern age is in a dangerous position, as they have been for the last decade the targets of Cyber weapons, and would be high targets of any invasion or malicious force. The research reviewed showed that various threats that Facilities face, from Stuxnet to foreign governments, and what standards are in place to secure these power generating plants. The authors agreed that proper safety and security checks where key to mitigating the risk of attack, and that a professional Security Audit goes a long way in securing Nuclear Facilities, thus finding the area of research to cover in the second part of this report.

4 References

1. Ahuja, L. Gupta, S. Rana, A. 2020. Security & Privacy Model for Work from Home Paradigm. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).* pp. 1351-1355.

2. Al-Rabiaah. 2018. The ". Stuxnet" Virus of 2010 As an Example of A "APT" and Its "Recent" Variances. *2018 21st Saudi Computer Society National Computer Conference (NCC).* pp. 1-5.

3. Akinlabi, S.A., Ayo, O.O., Ishola, F.A., Olatunji, O.O., Towoju, O. 2019. A Perspective Towards Sustainable Global Nuclear Security and Safety. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 02, FEBRUARY 2019.* pp. 92-96.

4. Greenberg, A. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* New York, Anchor Books.

5. Hellman, M.E. 2017. Cybersecurity, nuclear security, alan turing, and illogical logic. *Communications of the ACM, Volume 60, Issue 12.* pp. 52-59.

6. IEEE. 2021. IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations. *IEEE Std 692-2021.* pp. 1-57.

7. Kim, S., Kim, S., Kim, S., Kwon, K.H., Nam, K.H. 2019. Cyber Security Strategy for Nuclear Power Plant through Vital Digital Assets. *2019 International Conference on Computational Science and Computational Intelligence (CSCI).* pp. 224-226.

8. Litherland, P., Piggin, R., Orr, R. 2016. Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security. *11th International Conference on System Safety and Cyber-Security (SSCS 2016).* pp. 1-6.

9. Madnick, S. & Nourian, A. 2018. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing.* pp. 2-13.

10. United States Nuclear Regulatory Commission (U.S.NRC). 2013. *Nuclear Power Plant Security Assessment Guide.* Rockville, Office of Nuclear Security and Incident Response.

Other References:
FBI. 2020. Internet Crime Report 2020. Pennsylvania, United States of America. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [Accessed 31/10/2022]

PurpleSec. 2022. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022. [online] PurpleSec. Available at: https://purplesec.us/resources/cyber-security-statistics/ [Accessed 31/10/2022]

Singhm N. 2021. Cyber Crimes in India Spiked Nearly Nine Times Since 2013, UP Topped Chart in 2020: Data. [online] New 18. Available at: https://www.news18.com/news/india/cyber-crimes-in-india-spiked-nearly-nine-times-since-2013-up-topped-chart-in-2020-data-4210703.html [Accessed 17/11/2022]