From Water Plants to Nuclear Reactors: Mapping SCADA Vulnerabilities in Small Modular Energy Systems

Shreyas Kumar, Aleksander Alvarez, Jashanjodh Bajwa and Shrutwik Muppa
Texas A&M University, College Station, USA

shreyas.kumar@tamu.edu
alekalvarez@tamu.edu
jashanjodhb@tamu.edu
shrutwik@tamu.edu

Abstract: Supervisory Control and Data Acquisition (SCADA) systems are responsible for helping to manage a large portion of the industrial process, which keeps the economy running. In Small Modular Reactors (SMRs), SCADA helps with monitoring reactor conditions but is responsible for the careful variable control, which keeps reactors running optimally. Due to the far-reaching benefits of SCADA involvement, when there is a SCADA related attack, the consequences are also far-reaching. SMRs rely even more heavily on interconnected digital systems, meaning similar attacks could destabilize reactors, shut down industrial sites, or disrupt critical facilities such as refineries and military bases. This paper takes a closer look at SCADA vulnerabilities in the context of SMRs. Through analysis of the National Vulnerability Database, we compiled likely attacks on SMRs and evaluated them for threat severity and likelihood. Using trend analysis, topic modelling, and economic impact assessment, we show how these weaknesses could affect energy infrastructure and, more importantly, the many industries that rely upon it. Our findings underline the urgent need to strengthen the infrastructure defences, specifically in the realm of small modular nuclear reactors.

Keywords: Supervisory control and data acquisition, Industrial sabotage, Infrastructure protection, Modular nuclear reactors, Topic modelling

1. Introduction

Supervisory Control and Data Acquisition (SCADA) software has become increasingly implemented in industrial processes over time and, in the context of this study, is an integral part of the operation of Small Modular Nuclear Reactors (SMRs). SCADA software functions as the intermediary between human controllers and automated machinery and provides a platform to monitor and adjust variables in real-time. However, due to this integral role, vulnerabilities in SCADA software have great consequences for critical and sensitive infrastructure. A notable example of the potential far-reaching effects is a 2021 cyber-attack that occurred in Oldsmar, Florida. In the attack, the attacker attempted to exploit a simple remote access vulnerability to access a SCADA operator terminal in a water treatment facility, which could potentially have led to thousands of deaths (Davis, 2024). In nuclear reactors, SCADA is used to keep track of numerous variables that influence the fission and electricity-generating process and additionally coordinating between SMRs. SCADA monitors and adjusts these variables to keep the reactor stable and functioning optimally (Wang, 2024). To monitor and coordinate SMRs, increased numbers of digital devices will be needed, and these open pathways for attack (IAEA, 2023). With the growing popularity of SMRs, the cybersecurity issues become more urgent. This paper analyses SCADA vulnerabilities in the context of SMRs and explores their economic ramifications.

2. Related Work

Kaura, Sindhwani, and Chaudhary analysed the impact of cyber threats on SCADA systems and Industrial Control Systems. Focused on major real-world incidents such as Maroochy Water, Dragonfly, and TRITON. They introduced a three-tier system model: CAT-I, which involves direct damage in operations; CAT-II, attacks that cause potential disruption; and CAT-III, which focuses on espionage and low-level threats. The authors point out trends that include the rising role of state actors and the persistent APT campaigns. They emphasize the development of malware designed specifically for industrial control. The authors also mention phishing and social engineering as vulnerabilities on such systems. This is significant within the realm of SMRs due to the potential that the energy industry poses as an attractive target in widespread economic sabotage. In many of the uses of SMRs explored later such an attack would lead to great impact.

Daryabar et al. (2012) presented an extensive analysis of SCADA security from multiple threat sources such as insider actors, terrorists, malware developers, hackers, and hobbyists. SCADA systems are exposed as they rely on real-time functionality and wide-area connectivity, making them vulnerable to delays, disruptions, and unauthorized remote access that can directly impact critical operations. The authors stress the need for a solution for prolonged downtime as systems do not run due to their real-time nature. To mitigate such

vulnerabilities, the authors provide a couple of tests and advancements, such as red-team exercises, penetration testing, honeynet deployments, and stronger monitoring systems. Combining the measures provided by the authors would enable a protected and structured model.

3. Methodology

This study confronts the issue of SCADA vulnerabilities in relation to SMRs in a novel combination of various approaches.

3.1 Filtering

To quantify trend in vulnerability analysis, we rely on the National Vulnerability Database, which is an enriched list of CVE datapoints with CVE data combined with CVSS, CWE among other enriching data (NIST, n.d.). Common Vulnerability Scoring System CVSS is a standardized metric that provides a way to qualitatively understand a vulnerability's impact (NIST, 2022). Common Weakness Enumeration CWE is a collection of weakness categories that allows you to classify vulnerabilities by type (CWE, 2023).

To mine the data from the national vulnerability database, zip files containing the corresponding JSON files for 2014-2024 were used (nvd.nist.gov, n.d.). CVSS versions 2 and 3 was used. Through scripting, we identified data points related to SCADA through filtering vulnerability descriptions for keywords related to SCADA technologies. CWE, CPE, and CVSS information was then extracted from these entries.

3.2 Topic Modelling

To automate trend analysis in a way to find patterns hidden via the generalization of the CWE's vulnerability classification, topic modelling was applied to find common themes throughout Vulnerability Summary Text. First, this involved preprocessing steps that removed punctuation, stopping words and other non-descriptive common words. Then, this processed text data was plugged into a Latent Dirichlet Allocation (LDA) model. To maximize the quality of the LDA analysis for every year, a human supervisor finetuned parameters such as topic count and word count, leading to the results featured in our table.

3.3 Economic Analysis

To create an outlook for current market growth, the World Nuclear Association's database was analyzed for the status of all current SMRS. These results were filtered to only include the currently operational SMRs.

To examine the market outlook, the analysis was focused on the current quantity and quality of investments into SMR projects that had passed into the construction phase.

To create a model for the economic loss from nuclear reactors, data was acquired from the U.S. Energy Information Administration on the wholesale price of electricity. The number of reactors and total output in MWh in the U.S. was gathered from the World Nuclear Association to create an average output and gross profit figure per MWh.

The costs were incorporated by considering the three largest expenditures of fuel, capital, and operating costs. These costs were prioritized because they represent the bulk of the costs in SMRs. Smaller, miscellaneous expenses such as regulatory fees were not included in the costs, leading to an underestimation.

4. Results

4.1 SCADA Vulnerability Quantitative Trends

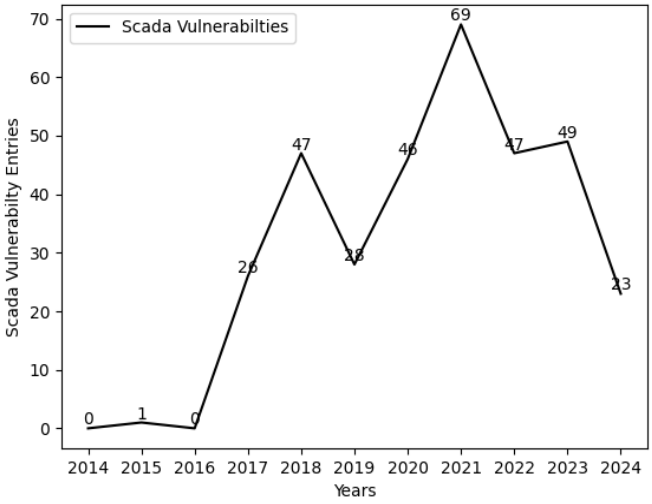

Figure 1: Increasing Trend in SCADA Vulnerabilities on the NVD

Figure 1. was created by calculating the number of SCADA vulnerabilities isolated per year. As seen from the graph, there is a general upward trend in vulnerabilities being identified as SCADA-based or SCADA adjacent vulnerabilities over the time of 2014 to 2024. There is a downward trend in vulnerabilities three times throughout the ten-year time but when comparing the start and end of the ten-year period, there is a definite trend upwards. Although compared to the total number of reported vulnerabilities in the national vulnerability database the SCADA-related vulnerabilities are quite small, the identified vulnerabilities are not trivial. SCADA vendors are relatively low in number, meaning that there are relatively few products that dominate the market meaning that the low number of vulnerabilities has a high impact. With the diversity featured in the different vulnerabilities, there is a significant risk to public infrastructure as well as energy generation.

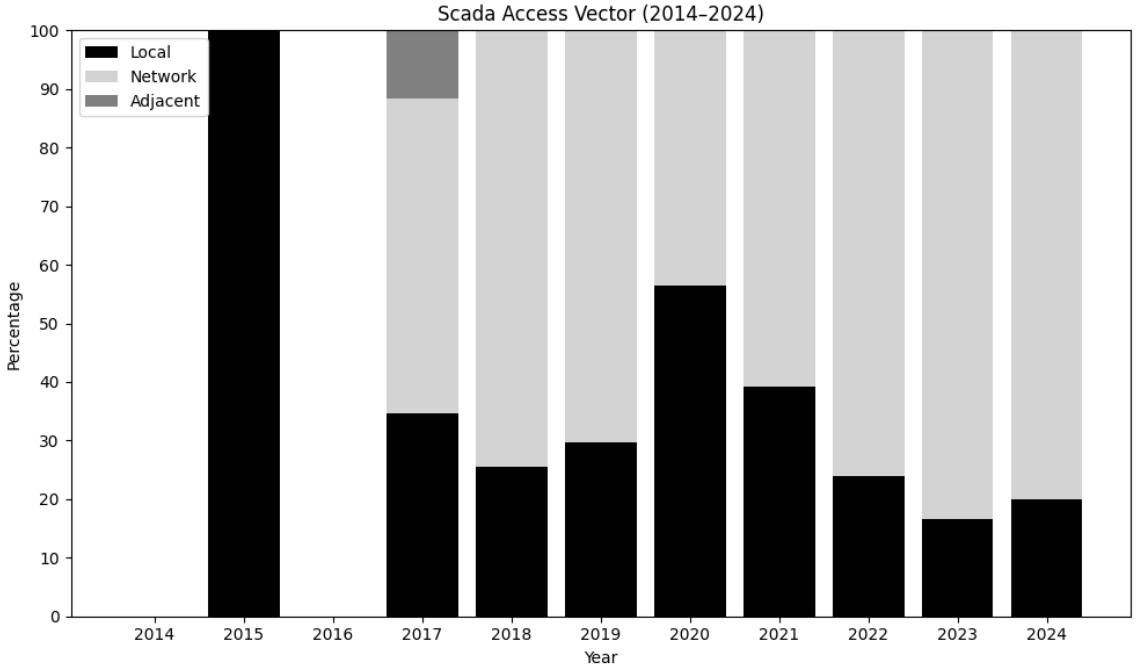

Figure 2: Attack Vectors of SCADA Vulnerabilities (2014-2024)

It is important to note from **Figure 1.** that there are several years where there is a low sample size, which is reflected in all trends drawn later. As seen from **Figure 2.**, the adjacent vector is the least prevalent vector type. This includes Bluetooth and attacks over the same network. What is most concerning with the case of modular nuclear reactors is network-based accounts, which happen to be the most common type of attack vector. Due to the nature of the use of modular nuclear reactors, most of them happen to be in very controlled environments where local attacks would only be possible if done by a previously authorized employee. While this certainly is a possibility that should be considered, the threat of a malicious remote hacker is one that should be the greater threat, as such an attacker would have anonymity and could reasonably cause havoc and potentially profit without consequence. Therefore, it makes it very concerning that these are the most common access vectors, which are remote. Combined with the prevalent categories for the Common Weakness Enumeration data, realistic possible attacks on modular nuclear reactors can be thought of and then planned. For example, with a hard-coded credentials vulnerability, a remote attacker could possibly sign in as an administrator remotely, thus potentially triggering safety measures that could affect reactor power output.

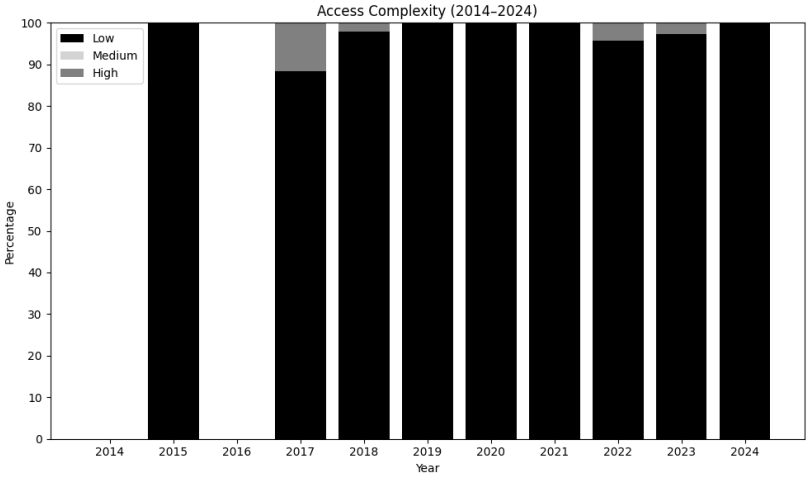

Figure 3: Access Complexity of SCADA vulnerabilities 2014-2024

From **Figure 3** all vulnerabilities are classified in three access complexity categories. Low complexity attacks pose a great security risk due to how they tend to be much easier to replicate, and these are unfortunately most common. For these reasons, they tend to be the vulnerabilities that have the maximum benefit in studying.

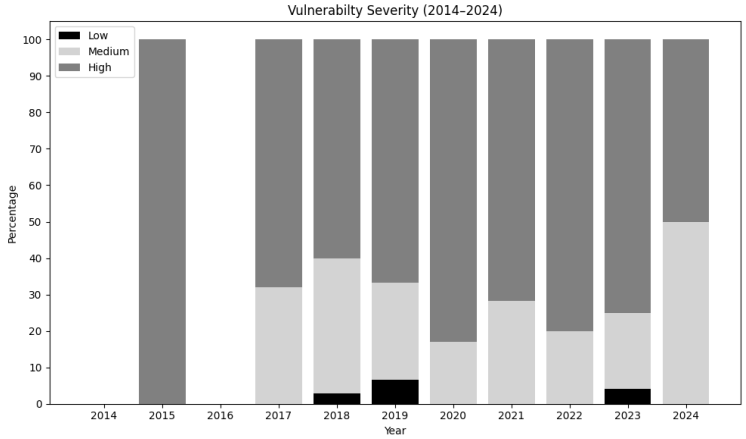

Figure 4: Vulnerability Severity 2014-2024

The National Vulnerability Database for its entries defines three scores to describe the severity risk, which is a standardized measure of the impact a vulnerability has on the user which interacts with it. In **Figure 4.** most vulnerabilities that are SCADA-related fall into the category of high severity. This is a concerning trend, as this metric is a measure of how the vulnerability affects the user. Since the user in this case is SCADA users, this means that most vulnerabilities in this field have a relatively high effect on these industrial systems. With the

application of SCADA software for remote monitoring and controls for modular nuclear reactors, the consequences of this trend are clear and quite important.

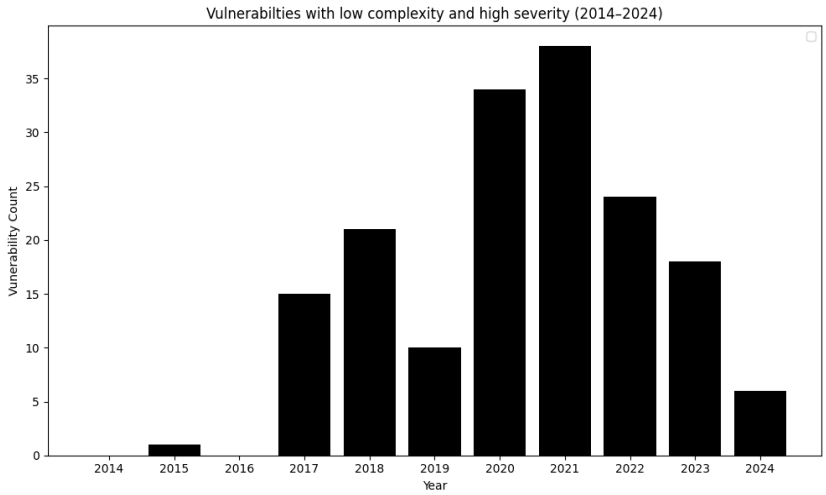

Figure 5: Trends of most serious vulnerability types 2014-2024

Vulnerabilities that are of prime importance are those whose complexity is low, along with a high severity.

From **Figures 1** and **5**, the trend with low complexity and high severity graph aligns closely with the SCADA in terms of the time figure. From this, the conclusion can be drawn that there tends to be around a certain percentage of vulnerabilities that are higher in severity and lower in complexity. This is significant because, as noted before, the low complexity vulnerabilities encourage a higher number of attacks before the solution to a vulnerability is found, and high severities increases the possibilities of consequences that malicious actors can implement on their targets. These vulnerabilities are the key ones that security professionals should analyze to create procedures and physical redundancies that can serve to immunize future reactors.

4.2 Categorical SCADA Vulnerability Analysis

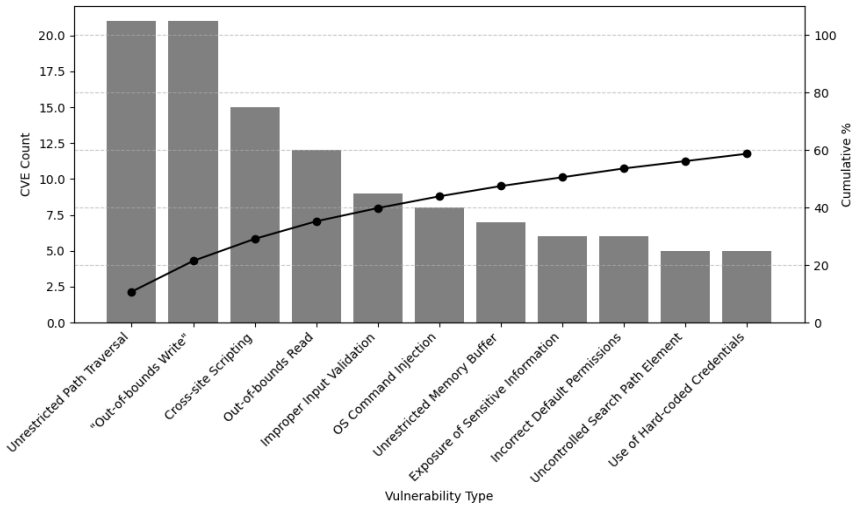

Figure 6: CWE Classification

Using the Common Weakness Enumeration data recorded in the NVD vulnerabilities, which were identified as SCADA-related vulnerabilities, the vulnerabilities were sorted by Category type. Using this sorted data, the Prevalent Categories graph was created. It is important to note that the noted category names are shortened forms of the CWE names. As seen from the graph, there is no one category with a clear domination of the dataset, yet there are some that are more prevalent than others. For example, the first eleven vulnerability categories, which are the ones featured in the graph, are the categories into which sixty percent of the recorded SCADA vulnerabilities fall into. The prevalence of some of these categories has obvious ramifications for Nuclear Reactors, as unrestricted path traversal regarding a SCADA system could lead to an attacker having

access to nearly all aspects of a remote system. Out of bounds write and out of bounds read both have similar implications, with out of bounds writes potentially leading to registers used by controlled devices being written two thus impacting the integrity of a SCADA system, for example parameters concerning reactor temperature could be changed, thus allowing an attacker to remotely cease a reactor's power production. For out-of-bounds read errors, this can affect the confidentiality of the information of the reactor. Such an attack could be used to steal admin credentials to enable a later system-critical attack on a SCADA energy system. One category with the lowest relative prevalence displayed on the graph is hard-coded credentialing, which, for obvious reasons, could lead to drastic consequences for modular nuclear reactors that utilize SCADA systems.

Table 1: Common Themes From Topic Modelling 2017-2020

2017	2018	2019	2020
Spider Control	Web Access Scada	Buffer Overflow	Local Execute
Directory Traversal	Remote Code Execution	Authentication	Directory Upgrade
Schneider Solutions	File Exfiltration	arbitrary reference	Installation Privilege
Uncontrolled Search	Disclosure	Denial of Service	IGSS
Cross Site Scripting	Authentication	Information Read	Remote Data Connect
Citect	Remote Port		Packet
Overflow Issue	Control Access		Server
Resource Consumption	Escalated Privilege's		Code Execution
	SQL Injection		User Authorization
	PLC Issue		Out of Bounds Read

Table 2: Common Themes From Topic Modelling 2021-2024

2021	2022	2023	2024
Signature Forge	User Privileges	Hardcoded Error	File Access
Endpoint Access	Buffer Overflow	SCADA Gateway	Firmware
Code Execution	User Authentication	File Overwrite	Code Injection
User Bypass	Input Validation	Code Execution	Logging
Passwords	Denial Of Service	Shell	User Authentication
Server Request		Certificate	
		Path Traversal	
		Plaintext Password Storage	

The value of the LDA Analysis can be seen in how quite a few of the captured themes overlap with the common CWE categories. This suggests that despite the limitations of the LDA analysis on smaller documents it still provides a reliable automated analysis. Additionally, there a more specific themes which would not have been captured by the CWE analysis such as specific attack vectors which shall prove to be valuable.

4.3 SMR Market Analysis

The current market of SMRs is quite small due to the relative recency of the technology, with only two operating reactors in China and Russia (World Nuclear Association, 2025a). This is changing rapidly, as billions are invested. The Korean SMR SMART 100 has been approved by Korea's Nuclear Safety and Security Commission in September 2024, after nearly 4 years of waiting (World Nuclear News, 2024). With the cost and risk associated with nuclear power in general, investments come in bursts, as was the case with the Darlington New Nuclear Project, which invested 15.1 billion USD into four SMRs at once. The reactors are to be built in phases, with the final reactor finishing in the mid-2030s. The cost of these reactors is also projected to be progressively cheaper as the new reactors are built, with the final being around 1/3 cheaper than the first (World Nuclear News, 2025). In comparison, the cost of Vogtle Units 3 and 4 in Georgia, United States, which are the latest reactors built in the United States, is estimated to be over 30 billion USD (U.S. Energy Information Administration, 2024). When comparing output, the investment is quite similar between the two

but the scalability for SMRs can be superior due to lower upfront capital costs, leading to a market advantage. The market of SMRs can be defined by the categories of geographical advantage, industry application, infrastructure requirements, and, most importantly, scalability (Gaster, 2025). The niche group of geography, industry, and infrastructure is the smaller share of the market where SMRs have the advantage of being able to supply remote areas, industrial needs for heat, or areas with poor infrastructure, instead of other energy options. The larger group is the scalability factor of SMRs for general electricity production (Lokhov, Cameron, Sozonuik, 2013). The advantage of being able to mass-produce reactors and interconnect them to create an easily scalable power plant is a huge advantage for SMRs. Thus, the market for SMRs is dependent on the extent to which this property is employed. While scalability has shown to decrease cost, the hindrances from time costs and initial investments may lead to slow implementation. There are currently over 80 SMRs in some phase of development, and the market outlook for SMRs is dependent on how many of these projects make it to fruition (International Atomic Energy Agency, 2025). SMR technology has immense potential, but its growth will only be realized in the coming decades.

4.4 Economic Loss Model

To estimate losses, we will look at the profits of the Average nuclear reactor and analyze the per-GWh profit. These numbers are based on the current U.S. market and nuclear capacity. There are currently 94 operable reactors with a total of 781,945 GWh of electricity generation in 2024 (World Nuclear Association, 2025b). Based on this, there is an average of 8318.56 GWh of electricity produced on average by each reactor per year. 22.79 GWh is produced every day, or 949.61 Megawatts per Hour. During 2024, the average sale price of wholesale electricity was $44.82 per megawatt-hour of electricity (U.S. Energy Information Administration, 2025). The prices vary by the energy market and when in the year they are sold, but we can take the average of all markets over all time, as we did with the nuclear capacity. With these numbers, we can come up with a gross income for the average reactor and by megawatt, but for profitability, we need expenses. There are several factors that can push profitability down, such as licensing fees, waste management, and other smaller costs. To simplify, we will focus on the big expense that includes fuel, capital costs, and operating costs. In the year 2023, the average cost in the U.S. for fuel was $5.32, for capital was $7.06, and for operating was $19.38 per MWh (Nuclear Energy Institute,2025). This gives us a total of $31.76 per MWh in costs. Now, to create a profit per MWh, we take out $31.76 of the average cost of electricity at $44.82 and get $13.06 in profit per MWh produced. To apply this to the average nuclear reactor in the United States currently, it would mean a profit of about $12,401.91 per hour or about $297,645.76 per day. These numbers are based on averages of both revenues and costs, so there will be an error in the calculations, and profit will be significantly higher for reactors who have already paid off their construction costs. Keeping this in mind, the profit will be significantly higher for some reactors.

4.5 Projected Losses for SMRs

As we have defined in earlier sections, one of the most important attributes of SMRs is their scalability. Though SMRs are typically rated up to 300MW, like the Korean SMART 100, the scalability allows for the potential for vast networks of SMRs working together. In the case of Canada's Darlington New Nuclear Project, 4 SMRs together would add up to 1200 MW of energy. This scalability also runs both ways when looking at the vulnerability of these reactors to cyber-attacks, especially SCADA. With the average nuclear reactor profiting nearly $300,000 a day, reactors being taken down are costly. This is only exacerbated by the scale at which SMRs might be deployed. If SMRs can reach the level of production that makes them competitive with other forms of power, security will need to be taken into even higher consideration. Though currently nuclear plants already have tight security procedures, the quantities involved in scaling SMR technology may require security to become even more rigorous. Thus, cyberattacks will have dire consequences as SMR scalability leads to plants having even higher outputs than the average reactor currently, leading to losses of magnitudes far greater than the $300,000 per day we might see today.

4.6 Scenario-Based Losses

Earlier sections provided a general estimation of losses from reactor downtimes in monetary terms. This section aims to look at specific scenarios and their impact and probability of occurrence but in relative terms. We will investigate how different vulnerabilities translate to physical action and economic impact relative to each other. We will not investigate exact probabilities, which can be difficult to quantify, and instead focus on relative estimations of common vulnerability types. We will choose one representative vulnerability from three tiers of likelihood. From **Figure 6**, path traversals are high likelihood, OS Command injections are medium likelihood, and hard-coded credential vulnerabilities are low likelihood. Economic impact can be highly varied,

even in specific cases. Thus, we will look at the broad impact and label tiers to the economic impact. Path traversal attacks aim to access files that are outside of the web root and can have varied consequences. The most extreme of these is the crash of the program, where the attacker can edit or delete critical files (Common weakness enumeration, 2024b). Depending on the criticality of the impacted system and the protections implemented, this vulnerability can range from no impact to shut down for long periods of time. This leads to a moderate economic impact, as the severity of vulnerability is not always critical. OS command injections, on the other hand, function through the lack of input validation. These attacks include the attackers adding their own code to be executed by the system (Zhong, n.d.). Like path traversal attacks, these vulnerabilities have a varied impact and share the same extreme of allowing for the deletion of files. Due to identical reasons, this vulnerability has the potential for moderate economic impact. Lastly, hard-coded credential attacks involve hard-coded passwords being used to gain access to a system (Common weakness enumeration, 2024a). This essentially leads to an attacker having privileged access to the complete system, depending on the credentials. Due to the span of access, this is the most critical vulnerability out of the three discussed. Correspondingly, this vulnerability can lead to the highest economic impact, as an attacker can create damage on a higher level of magnitude. Overall, these specific vulnerabilities vary in their probability of occurrence, but their economic impact is typically moderate to high.

5. Discussion

While the numerous aspects of this analysis have been done before, novel and actionable insights from this paper when a holistic view is taken. Through a combination of the NVD quantitative and qualitative analysis in addition to the economic analysis, a complete picture of the landscape to be combatted can be formed.

5.1 Overall Trends Analysis

The National Vulnerability Database Analysis period of 2014 to 2024 displays a concerning trend about SCADA vulnerabilities. From **Figure 1**. SCADA-related vulnerabilities have generally increased over this period. Although they comprise a small fraction of the total vulnerability count with how a large market share of SCADA services originate from very few companies (NERC), this trend should be cause for alarm. If most SCADA software's originate from relatively few companies, then a relatively small number of vulnerabilities, such as the ones studied in this paper, with a diverse range of origins, which can be seen in the vendors that pop up in the thematic analysis, will have wide reaching and concerning affects.

From **Table 1** as well as the CWE Categorical Classification, most vulnerabilities fall into the categories of Privilege Escalations and Code Execution. This second category is of great interest due to the high potential impact it has. Assuming all safety measures occur as planned, the worst-case scenario for remote code execution would be the temporary shutdown of the Reactor. For example, CVE-2019-10980 is one of the high severity low complexity vulnerabilities allowing project files to remotely execute code. Disregarding the secondary effects which a reactor shutdown would have, this could cost around $300,000 if turnaround time was less than a day, which is an unrealistic time frame. It would be advisable for nuclear SCADA software to separate data manipulation scripting from sensor reading to prevent customization on the part of the user as much as possible. This would decrease the risk of such a remote attack.

Through a combination of economic analysis, quantitative analysis, and categorical analysis, further headways in securing the future of Modular Nuclear Reactors can be made.

5.2 Privilege Escalations

From both the categorical analysis and the topic modelling, one persistent and common threat to SMRs is the category of privilege escalation. Beyond interfering with the operation of a modular nuclear reactor, this also poses a risk to the confidentiality of the plant's application. It is important to remember that many SMRs are intended for usage with critical industrial sites and military sites. In these applications, information regarding power usage has obvious value to cyber adversaries and thus is an additional impact that must be studied/considered.

Beyond information disclosure concerns, privilege escalation has measurable concerns when it comes to affecting the operational integrity of the SMR. The CWE analysis demonstrates quite a few categories relating to privilege escalation are of particular concern, and looking at the topic model, more specific themes to SCADA include SCADA gateways. When analysing vulnerabilities mined over the relevant time frame throughout the year 2023, a pattern of insecure privilege practices, which could pose great challenges to the operations of the SMR.

For example, CVE-2023-39460 would allow an attacker to potentially create an unauthorized file in the SCADA system. If, hypothetically, an attacker were to exploit this to create an executable capable of affecting reactor function this would have a greater than $300,000 impact.

From this pattern of vulnerabilities, it is advisable that for applications involving SMRs, practices of least privilege and non-customization should be adopted, thus strengthening the security of the system. Additionally, physical input should be required for actions that would result in a shutdown.

5.3 Vulnerabilities of Key Interest

Throughout this paper, vulnerabilities of note have been collected for their identifying characteristics of being both High in severity and low in complexity. It is this set that, when studied, it reveals pertinent answers regarding strengthening Modular Nuclear Reactors. One vulnerability to highlight is CVE-2024-10313. This vulnerability in SpiderControl SCADA allowed a malicious energy management system project template file to write files to arbitrary locations, which could lead to consequences such as overwriting files, system paralysis, or adversaries gaining remote control of equipment (NIST, 2024). With consequences of this severity, it is critical for fail-safes to be implemented and required across all reactors. A digital solution could include a virtual testing environment that analyses the file for arbitrary writes before clearing it. This is, however, not a full solution and would need to be used in conjunction with other safety protocols. Using a virtual machine (VM) can isolate the overwrites, but attackers may still cause damage if the VM is not used in a segmentation firewall, which isolates the VM from the rest of the network. These are some general measures that can be used to limit the impact of these vulnerabilities. While they are good practices, it is still crucial to maintain the latest cybersecurity measures, as attacks are constantly evolving.

5.4 Limitations

There are some important limitations that are important to note from this papers analysis.

As stated, before trends derived from the NVD are oftentimes and underestimate of the true landscape. This is because the National Vulnerability Database is dependent on voluntary reporting from researchers and developers. It is important to utilize the NVD as it remains the most reliable way to compare vulnerabilities across different platforms. Additionally, LDA analysis is known for having noisy results when done over small text datasets, but as seen in the similarities between some topics covered in the categorical analysis and the thematic analysis as well as how more pertinent trends to SCADA can be found using LDA it has its place in advancing this analysis.

As for the limitations of the economic analysis, it was mentioned before that several types of expenses for nuclear reactors are not included in the costs. This is due to the amount of variation and the weight of the miscellaneous expenses, such as fees. These expenses can vary between states and countries, which makes it difficult to account for all of them. The fact that these expenses are, comparatively, smaller than the three categories that are accounted for also reinforced the decision to omit these expenses. This does, however, make the costs an underestimate and the profits an overestimate. It is also important to note that in the process of creating an average of the wholesale price for electricity, this study simplifies the prices in several markets in the United States into a single average. This takes away some variation, and thus the study may not align completely with prices in different markets.

6. Conclusion

This paper presents a quantitative and qualitative assessment of the risk environment in which Modular Nuclear Reactors find themselves, in addition to an economic analysis to quantify these results. The quantitative analysis depicts an increasingly hostile environment where attackers can increasingly utilize network-based attacks to cause cyber terror at a distance. The qualitative analysis reveals a thematic emphasis on privilege escalation and its subsets. This has a specificity that would not be available relying solely on CWE categories. This, combined with the direct economic impact this has been shown to cause, is why action in this area is required.

6.1 Key Takeaways

For the developers of SCADA systems, which are used in Modular Nuclear Reactors, greater strengthening is needed around Permissions. These includes greater inclusions of Sandbox architecture as well as isolation of client-side scripting. For the integrators of SCADA with Modular Nuclear Reactors care should be taken to have physical redundancy for critical operations and sequences. If there is physical verification of certain actions

shut as reactor shutdown, then attacks would have to increase in sophistication. For research professionals' interest should be applied to computing the total indirect cost of this category of attacks, as well as vulnerability evolution.

Ethics declaration: As seen in Section 2 there were no human subjects, and all analysis was done on public data therefore no ethical board was required.

AI declaration: AI was not used throughout this paper besides the LDA analysis which we conducted.

References

CWE (2023). *CWE - New to CWE*. [online] cwe.mitre.org. Available at: https://cwe.mitre.org/about/new_to_cwe.html.

CWE (2024a). Common weakness enumeration. [online] cwe.mitre.org. Available at: https://cwe.mitre.org/data/definitions/798.html

CWE (2024b). Common weakness enumeration. [online] cwe.mitre.org. Available at: https://cwe.mitre.org/data/definitions/22.html

Daryabar, F., Dehghantanha, A., Udzir, N.I., Sani, N.F.M. and Shamsuddin, S.B. (2012) "Towards secure model for SCADA systems", *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. 312–317. [online] IEEE. Available at: https://doi.org/10.1109/CyberSec.2012.6246111 [Accessed 30 Sep. 2025].

Davis, R. and Keskin, O.F. (2024). "Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape." doi:https://doi.org/10.1109/sieds61124.2024.10534706.

Gaster, R. (2025) "Small Modular Reactors: A Realist Approach to the Future of Nuclear Power", [online], Itif.org, Available at: https://itif.org/publications/2025/04/14/small-modular-reactors-a-realist-approach-to-the-future-of-nuclear-power/.

Iaea.org. (2023). *Securing Digital Technologies of the Next Generation of Nuclear Reactors | IAEA*. [online] Available at: https://www.iaea.org/bulletin/securing-digital-technologies-of-the-next-generation-of-nuclear-reactors [Accessed 25 Aug. 2024].

International Atomic Energy Agency (2016) *Small Modular Reactors (SMR)*, [online], Iaea.org, Available at: https://www.iaea.org/topics/small-modular-reactors.

Kaura, C., Sindhwani, N. and Chaudhary, A. (2022) "Analysing the Impact of Cyber-Threat to ICS and SCADA Systems", *2022 International Mobile and Embedded Technology Conference (MECON)*, pp. 115–120. [online] IEEE. Available at: https://doi.org/10.1109/MECON53876.2022.9752425 [Accessed 30 Sep. 2025].

Lokhov, A., Cameron, R. and Sozonuik, V. (2013) *OECD/NEA Study on the Economics and Market of Small Reactors*, [online], Nuclear Engineering and Technology, 45, pp.701–706, doi: https://doi.org/10.5516/NET.02.2013.517.

NERC | Report Title | Report Date I Cyber Security Supply Chain Risks Staff Report and Recommended Actions. (2019). Available at: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20%2820190517%29.pdf [Accessed 26 Sep. 2025].

NIST (n.d.). *NVD - General*. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/general.

NIST (2022). *NVD - Vulnerability Metrics*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln-metrics/cvss.

nvd.nist.gov. (n.d.). *NVD - Data Feeds*. [online] Available at: https://nvd.nist.gov/vuln/data-feeds.

Nuclear Energy Institute (2025) *Nuclear Costs in Context*, [online], Available at: https://www.nei.org/CorporateSite/media/filefolder/resources/reports-and-briefs/2024-Costs-in-Context_final.pdf.

U.S. Energy Information Administration (2024) *Plant Vogtle Unit 4 begins commercial operation*, [online], Available at: https://www.eia.gov/todayinenergy/detail.php?id=61963.

U.S. Energy Information Administration (2025) *Wholesale Electricity and Natural Gas Markets Data*, [online], Available at: https://www.eia.gov/electricity/wholesale.

Wang, Y., Chen, W., Zhang, L., Zhao, X., Gao, Y. and Venkata Dinavahi (2024). *Small Modular Reactors: An Overview of Modeling, Control, Simulation, and Applications*. *IEEE Access*, pp.1–1. doi:https://doi.org/10.1109/access.2024.3351220.

World Nuclear Association (2025a) *Small Modular Reactor (SMR) Global Tracker*, [online], Available at: https://world-nuclear.org/information-library/current-and-future-generation/small-modular-reactor-smr-global-tracker.

World Nuclear News (2024) *South Korean SMR design approved by regulator*, [online], Available at: https://www.world-nuclear-news.org/articles/south-korean-smr-design-approved-by-regulator.

World Nuclear News (2025) *Canada's first SMR project: How is CAD20.9 billion cost calculated?,* [online], Available at :https://www.world-nuclear-news.org/articles/what-is-the-budget-for-canadas-first-smr-project.

World Nuclear Association (2025b) "United States of America – Reactor Database", [online], Available at: https://world-nuclear.org/nuclear-reactor-database/summary/United%20States%20Of%20America.

Zhong, W. (n.d.). Command injection. [online] OWASP Foundation. Available at: https://owasp.org/www-community/attacks/Command_Injection