ISSN: 3067-929X
Review Article

Journal of Electronics Science and Electrical Research

Enhancing Computer Security of Small Modular Reactors

Lilian MIHESO

University of Nairobi, Nairobi, Kenya

***Corresponding author:** Lilian MIHESO, University of Nairobi, Nairobi, Kenya.

Submitted: 05 January 2026 **Accepted:** 12 January 2026 **Published:** 19 January 2026

Citation: *Miheso, L. (2026). Enhancing computer security of small modular reactors. J of Electron Sci and Electrical Res, 3(1), 01-03.*

Abstract

Small Modular Reactors (SMRs), suitable for off-grid applications, offer more affordable and clean energy. One of the key obstacles to their implementation is accelerating technological development while maintaining compliance with safety and security standards throughout their lifecycle. This paper aims to address computer security challenges in the deployment of SMRs. SMRs rely heavily on digitalization, making them susceptible to cybersecurity threats that jeopardise their safety and functionality. Adequate measures must be put in place to mitigate the risk of insider threats, including employee training and strict access controls to limit access to critical systems and information. Regularly updating and patching software and systems can prevent Advanced Persistent Threats(APTs) from gaining long-term access. Encryption, multi-factor authentication, firewalls, and intrusion the detection systems protect communication channels from cyber threats. Establishing a well-defined emergency response plan, a data recovery plan and regular backup procedures ensures data integrity and provides a means to recover quickly from a cyber incident. Adopting a proactive and multidimensional cybersecurity approach reduces the risk of cyber threats and enhances the overall resilience of the nuclear infrastructure. Addressing these challenges requires a multi-faceted strategy involving collaboration between stakeholders, cybersecurity experts, and governments.

Keywords: Smrs, Computer Security.

Introduction

Small Modular Reactors (SMRs) are nuclear reactors that are smaller in size compared to traditional nuclear power plants. They are designed to be more flexible and cost-effective, making them suitable for a variety of applications, including industrial settings and as a complement to renewable energy sources. SMRs offer potential benefits such as enhanced safety features, reduced construction time and the ability to be manufactured off-site and be transported to the installation site. They are seen as a promising technology for addressing energy security, reducing greenhouse gas emissions, and meeting the growing energy demand.

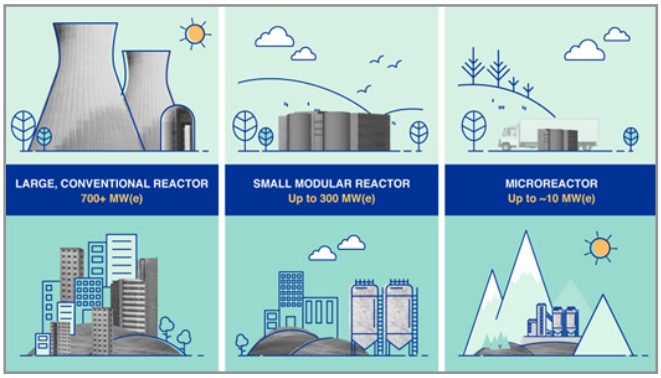

Figure 1: Small Modular Reactors (Image: A. Vargas/IAEA)

Critical national infrastructure is coming under more and more threat from cyberattacks. Cyberattacks on nuclear power plants have the potential to result in physical harm to the facility, disable its security or safety systems, grant unauthorized access to confidential nuclear data, or enable the illicit removal of radioactive material. For nuclear facilities to safeguard both nuclear security and nuclear safety, computer security is essential. Governments and businesses in the private sector are among the many stakeholders who have begun to adopt cybersecurity strategies. Maintaining the emphasis on security in a project as complicated as the construction of a small modular reactor is a huge issue, but recognizing and following best practices in cybersecurity would be a comforting and successful start to a new build. Senior project managers will certainly need to devote their entire attention to certain issues, including funding, sophisticated design and construction, hiring experts, and the effects of media, governmental, and public monitoring.It would make sense to not give priority to issues that need less immediate attention in the early stages of design, including protecting instrumentation control systems that might not be acquired for several years into the project. One of the key obstacles to the implementation of Small Modular Reactor technology is accelerating technological development while maintaining compliance with safety and security standards throughout their lifecycle. They rely heavily on digitalization, making them susceptible to cybersecurity threats that jeopardize their safety and functionality. The deployment of Small Modular Reactors in the context of computer security presents challenges that need careful consideration.

Challenges Arising from SMR Designs that Impact Computer Security:

Cybersecurity Threats: Increased digitalization makes SMRs susceptible to cybersecurity threats, such as hacking and malware that could compromise the safety and functionality of the reactors.

Supply Chain Vulnerabilities: Cyberattacks on suppliers or the supply chain could have cascading effects on the security of the entire SMR system.

Insider Threats: Insider threats, where individuals with access to critical systems intentionally or unintentionally compromise security, are a big challenge.

Remote Access Risks: The ability to remotely monitor and control Small Modular Reactors introduces the risk of unauthorized access from external networks.

Data Integrity and Privacy: Ensuring the integrity and privacy of sensitive data related to SMR operations is crucial. Unauthorized access or manipulation of data could impact the reliability and safety of the reactor.

Regulatory Compliance: Meeting cybersecurity standards and regulations is essential for the safe operation of nuclear facilities. Ensuring compliance with evolving cybersecurity standards and regulatory requirements poses an ongoing challenge.

Human Factor Challenges: Human errors and lapses in cybersecurity hygiene can contribute to vulnerabilities. Adequate training for personnel, strict access controls, and regular security audits are necessary to address human factor challenges.

Resilience to Advanced Persistent Threats (APTs): SMRs must be resilient to sophisticated and persistent cyber threats. Advanced Persistent Threats (APTs) pose a significant challenge, as they involve stealthy, continuous attacks with the aim of gaining long-term access to systems.

Securing Communication Networks: Communication networks that connect various components of SMRs must be secure. Encryption, authentication, and intrusion detection mechanisms are vital to protect against cyber threats on communication channels.

Emergency Response Planning: In the event of a cyber incident, having a well-defined emergency response plan is crucial. This includes strategies for isolating affected systems, restoring operations, and communicating with relevant stakeholders. Addressing these challenges requires a multi-faceted approach, involving collaboration between different stakeholders. Continuous monitoring, regular security assessments, and staying abreast of evolving cybersecurity threats are essential components of a comprehensive cybersecurity strategy for SMRs.

Measures to Address Computer Security Risks Associated with SMR Deployment:

Risk Assessment: To find potential weaknesses and dangers unique to the SMR system, a complete risk assessment should be done. Digital control systems, communication networks, and interfaces with external systems should all be taken into account in this study.

Regulatory Compliance: Verify compliance to pertinent cybersecurity laws and guidelines. Maintaining a strong cybersecurity posture requires adherence to established frameworks, such as those offered by international standards groups and nuclear regulatory bodies.

Secure Design and Development: Implement security by design principles during the development and design phases of the SMR. This includes integrating security features, minimizing attack surfaces, and conducting security reviews of the software and hardware components.

Network Security: Implement strong network security measures, including firewalls, intrusion detection and prevention systems, and network segmentation. Encryption protocols should be used to secure communication channels and protect against unauthorized access.

Access Control: Enforce strict access controls to limit access to critical systems and information. Implement the principle of least privilege to ensure that personnel have the minimum level of access necessary for their roles. This also helps by reducing the risk of insider threats.

Employee Training and Awareness: Provide cybersecurity training to all personnel involved in the Small Modular Reactor operations. The employees should be aware of common cyber threats and best practices for maintaining a secure working environment.

Patch Management: Regularly update and patch software and systems to address known vulnerabilities. Establishing a robust patch management process to ensures that the security updates are applied promptly.

Incident Response Planning: Develop and regularly test an incident response plan to effectively respond to cybersecurity incidents. This plan should include procedures for isolating affected systems, mitigating the impact, and communicating with relevant stakeholders.

Continuous Monitoring: Implement continuous monitoring of the systems for signs of unauthorized access, anomalous activities, or potential security incidents. Automated monitoring tools and intrusion detection systems can play a crucial role in this regard.

Security Audits and Penetration Testing: Conduct regular security audits and penetration testing to identify vulnerabilities and assess the effectiveness of security controls.

Secure Supply Chain Practices: Implement secure supply chain practices to ensure the integrity and security of components and software integrated into the SMR. This includes vetting suppliers and monitoring the supply chain for potential risks.

Collaboration and Information Sharing: Foster collaboration with other stakeholders in the nuclear industry, government agencies, and cybersecurity communities. Sharing information about emerging threats and best practices can enhance the overall security posture.

Backup and Recovery: Establish regular backup procedures and a robust data recovery plan. This helps provide a means to recover quickly in the event of a cyber incident.

Security Culture: Promote a strong security culture within the organization. Encourage a proactive approach to cybersecurity, where all employees understand their role in maintaining a secure environment.

Conclusion

The implementation of a comprehensive cybersecurity plan that incorporates many layers of defense is necessary to mitigate the computer security threats associated with the deployment of Small Modular Reactors (SMRs).Organizations deploying SMRs can lower the risk of cyberattacks and improve the nuclear infrastructure's overall resilience by implementing a multi-layered, proactive cybersecurity strategy. It's critical to update and modify cybersecurity protocols on a regular basis to keep up with changing dangers in the digital world. Addressing these challenges requires a multi-faceted approach, involving collaboration between nuclear industry stakeholders, cybersecurity experts, regulatory bodies, and relevant government agencies. Continuous monitoring, regular security assessments, and staying abreast of evolving cybersecurity threats are essential components of a comprehensive cybersecurity strategy for SMRs.

References

1. Brunt, R., Unal, B. (2019). Cybersecurity by design in civil nuclear power plants. Chatham House.https://www.chathamhouse.org/sites/default/files/2019-07-23-Cybersecurity-Nuclear-Power-Plants.pdf
2. Duguay, R. (2020). Small modular reactors and advanced reactor security: Regulatory perspectives on integrating physical and cyber security by design to protect against malicious acts and evolving threats. International Journal of Nuclear Security, 7(1), Article 2. https://doi.org/10.7290/ijns070102
3. Frick, K., Doster, J., Bragg-Sitton, S. (2018). Design and operation of a sensible heat peaking unit for small modular reactors. Nuclear Technology.
4. International Atomic Energy Agency. (2021). Computer security techniques for nuclear facilities (NSS-17-T, Rev. 1). IAEA. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf
5. Lei, Y. (2019). Assessing cyber security in small modular reactors. Canadian Nuclear Safety Commission. https://nuclearsafety.gc.ca/eng/resources/research/technical-papers-and-articles/2019/assessing-cyber-security-smrs.cfm
6. Organisation for Economic Co-operation and Development Nuclear Energy Agency. (2021). Small modular reactors: Challenges and opportunities (NEA No. 7560). OECD Publishing. https://www.oecd-nea.org/upload/duntocs/application/pdf/2021-03/7560_smr_report.pdf
7. Tan, S., Cheng, S., Wang, K., Liu, X., Cheng, Wang, J. (2023). The development of micro and small modular reactors in the future energy market. Frontiers in Energy Research, 11, Article 1149127. https://doi.org/10.3389/fenrg.2023.1149127