SIMULATING SMALL MODULAR REACTOR CYBERSECURITY

Michael B. Zamperini
mbzamperini@liberty.edu

ABSTRACT

This study proposes methods of computer simulation to study and optimize the cybersecurity of Small Modular Nuclear Reactors (SMRs). SMRs hold potential to help build a clean and sustainable power grid but will struggle to gain widespread adoption without public confidence in their security. SMRs are emerging technologies and potentially carry higher cyber threats due to remote operation, large numbers of cyber-physical systems, and low on-site personnel staffing. Computer simulations using agent-based modeling approaches have shown promise in studying existing cybersecurity frameworks. Methods of agent-based computer simulations to test improved methods of collaboration between power plants and cybersecurity vendors can strengthen SMR cybersecurity as these new power generators make their way into the market. Employing simulation to heighten cybersecurity will help to safely leverage the potential of SMRs in a modern and low-emission energy grid.

Keywords: cybersecurity, simulation, agent-based modeling, small modular reactors, common criteria.

1 PROPOSAL

In our post-September 11th world, security must always be vigilantly considered. When considering the cyber security of nuclear energy installations, the potential costs of successful cyber-attacks are extreme. Whether outcomes include the release of nuclear contamination or theft of nuclear material, nuclear cybersecurity must be as close to perfect as possible. The assessment of cybersecurity in new technologies such as Small Modular Nuclear Reactors (SMRs) can be especially challenging. Computer simulation that explores the randomness of cyber-attacks and cyber defense systems is a powerful tool to maximize cybersecurity plans and probe potential weaknesses.

Computer simulation has been used to evaluate cybersecurity, but the research is still relatively underdeveloped. A recent literature review searched for research on cyber-attack simulations over the past 20 years [1]. Starting with keyword searches, hundreds of papers were sifted to narrow the search down to 11 pieces of research that met strict definitions of computer simulations and cyber-attacks. Of these 11 papers, six were based on discrete event simulation methods while only two made use of agent based modeling (ABM). ABM may prove more useful in mimicking the complexity of the dynamics of stakeholder behavior in a cyber-attack, yielding more realistic models that could highlight emergent conditions of which cyber planners and designers should be aware.

One area in which ABM can be useful with emerging SMR cybersecurity concerns is through the Common Criteria (CC). The CC website describes itself as an international collaborative organization working to coordinate the creation of secure information technology products that are tested and recognized by the member nations and organizations [2]. Essentially, nuclear stakeholders can use the CC to enumerate their cyber needs seeking verified and recognized solutions. The International Organization for Standardization categorized CC security problems as open threats in need of a technical solution [3]. Cyber threats should be defined as clearly as possible so that resulting evaluations and proposed solutions can address the right problem. Agents modeled in ABM can learn and adapt over the course of a simulation,

Proc. of the 2024 Annual Simulation Conference (ANNSIM'24), May 20-23, 2024, American University, DC, USA
P.J. Giabbanelli, I. David, C. Ruiz-Martin, B. Oakes and R. Cárdenas, eds.

along with forming coalitions with other agents. These characteristics of ABM can be leveraged to model the effect of the CC on the evolution of cybersecurity in the nascent stages of SMR development.

When analyzing a new technology such as SMRs, it is helpful to consider how the cybersecurity profile may be different from other comparable existing systems. With SMRs being constructed off-site at an assembly plant, the supply chain of the parts could introduce cyber vulnerabilities [4]. If SMRs rely on more use of digital systems to control physical systems, successful cyberattacks could affect the physical security of the reactor. Certainly, increased remote operation of SMRs will introduce more cyber risks. If SMRs have minimal on-site workers, the stake of an insider cyberattack could be much higher. Adding to these considerations, SMR installations are being widely considered to provide not just electricity but also heat for various industrial applications. These notions of having SMRs digitally connected with other industrial, or energy production systems also introduce additional potential sources of cybersecurity weaknesses.

Past research has employed an ABM of a hypothetical zombie apocalypse to demonstrate the capabilities of this simulation paradigm [5]. This model can be customized to simulate cybersecurity applications. In the zombie apocalypse model, agents were either zombies or humans. For cybersecurity, agents can be either well-intentioned or nefarious actors. The zombie model can be used to explore interventions that could save humans from zombies. A cybersecurity version can search for conditions that thwart attackers. The zombies can be programmed to move fast, or slow, as cyber attackers and network users can be initialized with advanced or low-level hacking or defense skills. Human agents can be set to fight or flee from zombies, as computer users can be programmed with different methods of dealing with cyber attackers. The zombie apocalypse may seem like a fun way to demonstrate ABM capabilities, but the apocalypse model can be extended to other applications such as cybersecurity.

Cybersecurity can benefit from computer simulation studies, both for existing applications and new proposals such as SMR power generation installations. The use of stochastic simulation to study cybersecurity can be found in the existing research but is still in its early stages. ABM offers intriguing simulation options that could be well suited to cybersecurity and the particular cyber needs of nuclear power plants and new SMR technologies. The ability of agents in an ABM to interact with one another and learn as a simulation run progresses fits well for cybersecurity modeling. The Common Criteria framework through which cybersecurity users can list their open needs, coordinate with vendors to create solutions, and obtain certification of these solutions from independent laboratories is deserving of exploration through ABM simulations. Such studies have the potential to illuminate future cybersecurity scenarios that have not been considered, informing and strengthening cyber defense and contingency planning strategies.

ACKNOWLEDGMENTS

Dr. Name is the advisor for this research and has been influential in shaping the direction.

REFERENCES

[1] Engström, V., & Lagerström, R. (2022). Two decades of cyberattack simulations: A systematic literature review. *Computers & Security*, *116*, 102681. https://doi.org/10.1016/j.cose.2022.102681.

[2] Common Criteria. (n.d.). The Common Criteria. https://www.commoncriteriaportal.org/, accessed 10th January 2024.

[3] International Organization for Standardization. 2022. ISO/IEC 15408 Information Security, Cybersecurity and Privacy Protection. https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html, accessed 10th January 2024.

[4] Aamoth, B., Lee, W. E., & Ahmed, H. (2022). Net-Zero Through Small Modular Reactors-Cybersecurity Considerations. In IECON 2022–48th Annual Conference of the IEEE Industrial Electronics Society (pp. 1-5). IEEE. https://doi.org/10.1109/IECON49645.2022.9968304.

[5] Macal, C. M. (2018, December). Tutorial on agent-based modeling and simulation: ABM design for the zombie apocalypse. In 2018 Winter Simulation Conference (WSC) (pp. 207-221). IEEE. https://doi.org/10.1109/WSC.2018.8632240.