INL/CON-24-77554-Revision-0

Operation and Security Considerations for Heat Pipe Cooled Microreactors

June 2024

Ilyas Yilgor, Piyush Sabharwall, Scott E Ferrara

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-77554-Revision-0

Operation and Security Considerations for Heat Pipe Cooled Microreactors

Ilyas Yilgor, Piyush Sabharwall, Scott E Ferrara

June 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Operation and Security Considerations for Heat Pipe Cooled Microreactors

Ilyas Yilgor*, †, Piyush Sabharwall*, Scott Ferrara*

*Idaho National Laboratory, Idaho Falls, ID
†Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute, Troy, NY

[leave space for DOI, which will be inserted by ANS]

INTRODUCTION

Microreactors and small modular reactors (SMRs) are anticipated to be key elements in the carbon-free energy portfolio of the United States (U.S.), serving as reliable power sources for remote communities, disaster relief zones, extraterrestrial deployments, and backup power needs. They provide considerably low power outputs in the kilowatt to lower megawatt range (0.1 – 50 MWe), along with an incredibly compact form factor.

Microreactors employ technologies that are substantially more advanced and recent compared to conventional reactors. Furthermore, they are of a drastically smaller scale and are designed to be operated in a diverse set of locations, offering operational flexibility and mobility. In addition, the autonomous or semi-autonomous operation of microreactors with minimal or no on-site staff is anticipated. These factors give rise to specific challenges with regards to their safety and security. National and international regulatory agencies normally regulate many aspects of the security of a nuclear power plant (NPP). However, these requirements are being revised and improved for their applicability to microreactors [1,2]. Ensuring the security of microreactors is crucial for their cost-effective, timely, and safe deployment.

For these reasons, recent work has proposed to integrate security considerations in the design process of microreactor development to optimize designs and prevent cost overruns [3]. Although numerous microreactor designs exist, heat pipe cooled microreactors (HPMRs) offer unique advantages regarding safety, modularity, and mobility. HPMRs are characterized by their use of alkali metal heat pipes to transfer heat from the reactor core to the power conversion system [4]. Heat pipes are passive two-phase heat transfer devices that employ the cyclic evaporation and condensation of a working fluid to transfer heat between two interfaces [5,6]. The adoption of passively operating heat pipes as a core cooling solution enables improvements in terms of reactor's safety, reliability, and spatial footprint. However, the security implications of heat pipe use need to be robustly established.

Security considerations in the context of an HPMR can be broadly distinguished as physical [7], cyber/cyber-physical [8], operational, and material control and accounting related threats [9]. Among these, the present work investigates considerations related to heat pipe operation, reactor transport, and cyber/cyber-physical security to ensure the indirect and direct consequences of the actions of nefarious actors are understood and can be mitigated by design or through physical or cybersecurity measures. In addition, future directions are proposed for consideration by both HPMR designers and for regulators.

SECURITY CONSIDERATIONS FOR HPMRS

Security considerations related to HPMRs and other microreactors would largely depend on their use case and siting. For instance, those operating under remote or extensively monitored sites such as mines may require drastically different considerations compared to HPMRs powering disaster relief zones or densely populated regions. The differences could be in the aim, type, and sophistication of security threats. The distinct nature of each planned operating site could require unique licensing paths by regulatory agencies for specific applications.

Traditional design-basis threats (DBTs), as well as methods to mitigate or quantify the effects of such threats, could be relatively similar to other conventional or advanced reactors for civilian and commercial applications. Existing tools and expertise could be modified to adapt to the requirements of HPMRs, especially in the case of physical protection systems (PPSs) design and probabilistic risk assessment (PRA) tools [10]. However, the increased risk of cyber threats due to the use of modern technologies should be considered. Overall, technologies that make microreactors mobile and operationally flexible must meet or exceed existing safety and security standards of conventional NPPs. Current regulations may help form a guideline on these standards, however they currently do not offer clear objectives applicable to highly mobile reactors [11].

Heat Pipe Operation

Multiple HPMR designs have been proposed in literature. [12-15]. These designs employ various approaches with respect to their purpose, size, choice of fuel, choice of power conversion system, etc. However, their operation includes heat pipes that transfer the heat from the reactor core to the power conversion system, which is the main characteristic of HPMRs. Therefore, many concerns related to their safety and security can be expected to be common.

The main constraint on a heat pipe's performance can be identified as its operating limits [16,17]. Conventional heat

pipe analysis considers multiple limits that include the viscous, sonic, entrainment, capillary, and boiling limits. The limit for a particular case depends on the heat pipe geometry, wick structure, working fluid, and operating conditions. Limits being reached during operation may severely affect a heat pipe's power throughput, especially under evaporator dry-out conditions that could be observed under capillary, entrainment, and boiling limits. Furthermore, the failure of multiple heat pipes in removing core heat could cause a cascading effect which could result in the failure of additional heat pipes. However, reactors may be effectively designed considering this failure mode where adjacent heat pipes can adopt the power increase without failure [18].

Since heat pipes are passive devices, they can normally only be manipulated via their evaporator and condenser conditions. Therefore, an indirect attack to a reactor's heat pipes could involve the control of the power input and output to the heat pipes. This could be in the form of a hijacking of the reactivity control or power conversion systems to perform unsafe control actions [19]. Reactor thermal power being increased from nominal design levels, or the failure of the power conversion system, could cause higher failure probabilities for the heat pipes as they might operate closer to their operating limits. Upon the failure of multiple heat pipes, the reactor might experience significantly higher temperatures and temperature gradients which could cause damage to components due to increased mechanical and thermal stresses. An increase in the heat removal rate from the heat pipes could also cause undesirable effects such as unexpected coolant outlet temperatures, the reduction of the heat pipe operating temperature, and the flooding of the wick in the condenser.

The reactor could be at an increased risk of attack during transients such as startup and shutdown. The reactor power ramp rate during the startup process must consider the viscous, sonic, and frozen startup limits, which are significant at lower operating temperatures observed during startup. A ramp rate higher than what was designed could result in the rapid increase of core temperature which could result in structural damage to both the core and the heat pipes. Similarly, a high cooling rate during shutdown could also result in structural damage due to larger thermal gradients. Lastly, depending on the type of power conversion system, a high cooling rate during shutdown could cause the working fluid to freeze outside the evaporator region which could considerably affect the future startup performance of the reactor.

It should be noted that any sort of significant physical breach of the heat pipe casing could rapidly render the heat pipe inoperable. Heat pipes usually operate at pressures that are less than atmospheric, which means moisture could enter the heat pipe and potentially cause a fire as the surrounding fluid comes into contact with the alkali metal (working fluid). In addition, after the pressure is equalized with ambient, the working fluid could be lost in vapor form to the surroundings, which could result in additional safety hazards.

Reactor Transportation

Security risks can be particularly amplified during transportation through either densely populated areas or otherwise dangerous territories. Based on the recommendations given by Moe [11], the transportation of spent nuclear fuel and other high-activity shipments require the following physical security features:

1. U.S. Nuclear Regulatory Commission (NRC) certified shipping methods where the fuel is in non-dispersible form
2. Local law-enforcement support along routes if available
3. Protection of information related to the transport operation
4. Communication between the convoy and control centers
5. Additional armed escorts within densely populated areas
6. Vehicle immobility features to recover hijacked cargo with help from response forces

Furthermore, the transportation of previously operated microreactors will by itself necessitate a Type B package as designated by U.S. Department of Transportation (DOT)/NRC regulations. This means that either the microreactor needs to be housed in Type B packaging, or the reactor itself needs to be a Type B package [11], which must pass certain testing criteria for certification-including free drop, puncture, thermal, and immersion tests, respectively.

Cybersecurity

Microreactor designs are expected to utilize automated control systems consisting of modern digital components. In fact, many designs proclaim autonomous or semi-autonomous operation capabilities. Due to the small power outputs of microreactors, a certain level of automation and remote operation/monitoring capabilities are required to reduce operational staffing levels in order to strengthen economic feasibility [20]. Thus, reduction of vulnerabilities related to the proper operation of autonomous systems, particularly those related to reactor safety systems, is of paramount importance in heat pipe microreactors.

Digital systems are vulnerable to cyber-attacks unlike legacy analog systems, and they are also prone to malware and other malicious activities that could affect other systems in the network. Cyber threats to heat pipe microreactors could be in the form of malware (e.g., viruses, worms, trojans, and rootkits), human error, remote access, and advanced persistent threats which might affect reactor systems in a variety of damaging ways. The form and sophistication of attacks could depend on the type of digital system, its dependance on physical instrumentation and control systems, and its degree of automation.

HPMRs feature simplified and standardized modular designs that are manufactured in factories. Although this

approach enables reduced incidence of manufacturing errors [21], standardization also necessitates the integration of uniform digital systems on standardized software platforms which could enable adversaries' increased familiarity with systems present. Furthermore, more complex systems are usually more prone to contain errors which could be exploited. Therefore, rigorous cybersecurity measures for both external and internal threats must be employed as a part of the design of microreactors.

Instrumentation and control components are particularly prone to attacks since they receive signals and interact with physical systems that could be critical to the operation of a reactor. For instance, the hijacking of a control loop regulating important parameters such as temperature, pressure, or flow rate could seriously compromise safe reactor operation. Although the core is cooled passively in HPMRs, the malicious manipulation of such control parameters could force the system to operate outside heat pipe design conditions which could result in increased or non-uniform core temperatures.

Cybersecurity regulations are currently in place for existing NPPs; however, they must be adapted to consider the unique threats associated with these novel technologies. Sabharwall et al. presented a review of the cybersecurity concerns, threat identification, and threat mitigation strategies that are relevant to microreactor technologies including HPMRs [22]. They proposed recommendations for future research based on concepts such as autonomous cyber-defense systems and digital twins that could utilize artificial intelligence and machine learning.

To address these threats, multiple potential cybersecurity solutions are proposed by Sabharwall et al. [22]. that includes:

1. Commercial grade or stronger encryption schemes
2. Wireless signal shielding and highly directional signals
3. Segmented wireless connections
4. Use of one-way connections
5. Automated intrusion detection systems
6. Autonomous cyber-defense systems
7. Evaluating vulnerabilities and developing threat mitigation steps via digital twining
8. Use of semi-autonomous instead of fully autonomous control systems that allow human intervention during perceived attacks
9. Regularly updated anti-malware software
10. A robust network of security checks and gates to prevent unauthorized access
11. Proper cybersecurity habits by employees
12. Promoting cooperative engagement of microreactor manufacturers, government agencies, and international organizations against cyber-threats

The safety and reliability of microreactors are integral both for their utility and for the future of the nuclear energy sector at large. The solutions presented above may be employed starting from the design phase to enable increased cybersecurity for microreactors. An assessment hub based on the proposed solution was realized by Sabharwall et al. [22], where a digital twin, control feedback, and human operator are integrated alongside a nearly autonomous control system.

CONCLUSIONS

The rapid deployment and adoption of HPMRs require security considerations due to their compact sizes, distinct applications, and operational flexibility. The present work highlights certain security challenges related to heat pipe thermal hydraulic operation, reactor transportation, and cybersecurity. Future work should include experiments based on identified challenges on heat pipe operation to better quantify associated risks, considering the diverse operational capabilities of HPMRs.

ACKNOWLEDGEMENTS

This work builds on a critical first steps advanced reactor research project that was funded by the National Nuclear Security Administration (NNSA).

REFERENCES

1. B. B. CIPITI et al., "Advanced Reactor Safeguards: 2022 Program Roadmap," United States, SAND2022-11143R, (2022).
2. E. S. FLEMING LINDSLEY, M. NYRE-YU, and D. L. LUXAT, "Human Factors Considerations for Automating Microreactors," United States, (2020).
3. A. EVANS et al., "U.S. Domestic Microreactor Security-by-Design," United States, SAND2021-13779R, (2021).
4. I. YILGOR et al., "Recent Developments and Findings of Heat Pipe Experiments for Microreactor Applications," *Nuclear Technology*, (2024).
5. I. YILGOR and S. SHI, "Scaling laws for two-phase flow and heat transfer in high-temperature heat pipes," *International Journal of Heat and Mass Transfer*, **189**, pp. 122688 (2022).
6. S. SHI et al., "A two-phase three-field modeling framework for heat pipe application in nuclear reactors," *Annals of Nuclear Energy*, **165**, pp. 108770 (2022).
7. A. EVANS, J. L. RUSSELL, and B. B. CIPITI, "New Security Concepts for Advanced Reactors," *Nuclear Science and Engineering*, **197**(sup1), pp. S70-S79 (2023).
8. R. FASANO et al., "Cyber-Physical Risks for Advanced Reactors," Sandia National Laboratory, Albequerque, NM, SAND2021-11995, (2021).
9. B. CIPITI, "U.S. Domestic Material Control and Accounting for Advanced and Small Modular Reactors," Sandia National Laboratory, Albequerque, NM, SAND2022-11303C, (2022).
10. R. CHRISTIAN et al., "A Dynamic Risk Framework for the Physical Security of Nuclear Power Plants," *Nuclear Science and Engineering*, **197**(sup1), pp. S24-S44 (2023).

11. W. L. MOE, ″Key Regulatory Issues in Nuclear Micro-Reactor Transport and Siting,″ Idaho National Laboratory, Idaho Falls, ID, INL/EXT-19-55257, (2019).
12. D. I. POSTON et al., "KRUSTY Reactor Design," *Nuclear Technology*, **206**(sup1), pp. S13-S30 (2020).
13. J. W. STERBENTZ et al., ″Preliminary Assessment of Two Alternative Core Design Concepts for the Special Purpose Reactor,″ Idaho National Laboratory, Idaho Falls, ID, INL/EXT-17-43212, (2017).
14. M. M. SWARTZ et al., "Westinghouse eVinci™ Heat Pipe Micro Reactor Technology Development," *Proceedings of the 2021 28th International Conference on Nuclear Engineering*, (2021).
15. U.S. NUCLEAR REGULATORY COMMISION. *Combined License Application Documents for Aurora – Oklo Power Plant Application*. 2022.
16. A. FAGHRI, *Heat Pipe Science and Technology*: Global Digital Press (1995)
17. I. YILGOR, E. LAN, and S. SHI, "Design and Thermal-Hydraulic Performance Analysis of a Low-Temperature Heat Pipe Test Facility," *Nuclear Science and Engineering*, **197**(5), pp. 753-770 (2023).
18. V. J. LAWDENSKY et al., ″Effects of Heat Pipe Failures in Microreactors,″ Los Alamos National Laboratory, Los Alamos, NM, Los Alamos National Laboratory, (2020).
19. F. ANTONELLO, J. BUONGIORNO, and E. ZIO, "Insights in the safety analysis of an early microreactor design," *Nuclear Engineering and Design*, **404**, pp. 112203 (2023).
20. P. RAMUHALLI and S. M. CETINER, ″Concepts for Autonomous Operation of Microreactors,″ United States, ORNL/TM-2019/1305, (2019).
21. A. ABOU-JAOUDE et al., ″An Economics-by-Design Approach Applied to a Heat Pipe Microreactor Concept,″ Idaho National Laboratory, Idaho Falls, ID, INL/EXT-21-63067, (2021).
22. P. SABHARWALL et al., "Cyber security for microreactors in advanced energy systems," *Cyber Security: A Peer-Reviewed Journal*, **4**(4), pp. 345-367 (2021).