IDENTIFYING SABOTAGE RISKS AND ADVERSARIAL THREATS TO PASSIVE DECAY HEAT REMOVAL SYSTEMS IN ADVANCED NUCLEAR REACTORS

DARIUS LISOWSKI, MATTHEW BUCKNOR, DAVE GRABASKAS
Argonne National Laboratory, Lemont, IL. USA
email: dlisowski@anl.gov

SCOTT FERRARA, CHRISTOPHER CHWASZ
Idaho National Laboratory, Idaho Falls, ID. USA

DOUGLAS OSBORN
Sandia National Laboratories, Albuquerque, NM. USA

ALEX HUNING
Oak Ridge National Laboratory, Oak Ridge, TN USA

Abstract

Advanced and small modular reactors, including GenIV, aim to enhance reliability by incorporating passive safety systems into their plant design. These systems leverage passive methods to provide a high level of reliability for removing decay heat from the reactor core to achieve safe shutdown conditions or other safety functions. Since these systems, in some advanced reactor designs, could provide an ultimate heat sink for decay power, they could also serve a critical safety function. Given these systems' reliance on passive methods, they may present novel security risks and potential unique vulnerabilities to sabotage of nuclear facilities by insider threats and external adversarial attacks. Historically, evaluation of acts of indirect sabotage focused on primary threats to active system disruption or seizure, while considerations for passive systems (if present), were secondary. Thus, at the current time, there is limited existing literature on the threats unique to passive systems.

The paper presents a status and summary of an on-going project tasked with identifying the envelope of possible security threats to passive decay heat removal systems in advanced reactors. The project's goals are to determine which threats are most credible and realistic, assess these threats for their potential consequences on reactor safety, and establish recommendations to address the identified security concerns. Included in this paper is a narrative of the approach and methodologies to support threat determinations by others such as reactor developers and relevant stakeholders. Results and findings of the project will be documented separately in a full report once the overall project is completed later this year and issued to allow broad dissemination of the knowledge gained.

1. INTRODUCTION

Advanced nuclear reactors, including advanced small modular reactors (aSMRs) and Generation IV designs, prioritize enhanced reliability by integrating passive safety systems into their plant designs. These systems leverage passive methods to ensure the reliable removal of decay heat from the reactor core, ultimately achieving and maintaining safe and stable conditions. With robust designs, these passive safety systems become integral components of the nuclear power plant, often requiring no additional support systems nor human intervention during postulated and credible accidents [1].

Various advanced reactor designs, such as Molten Salt Reactors (MSRs), High Temperature Gas Reactors (HTGRs), Sodium Fast Reactors (SFRs), and Integral Pressurized Water Reactors (iPWRs), incorporate diverse approaches and technologies for decay heat removal. These include systems like the Reactor Vessel Auxiliary Cooling System (RVACS), Reactor Cavity Cooling Systems (RCCS), Direct Reactor Auxiliary Cooling System (DRACS), freeze plugs, and passive injection. In recent years, there has been renewed interest in aSMR designs, leading many vendors to actively develop reactor concept designs that incorporate one or more passive decay heat removal technologies [2, 3].

However, despite their high decay heat removal performance, these aSMR designs can also pose unique security challenges due to their increased reliance on passive safety features [4]. Therefore, the results from this research aim to provide reactor developers with the necessary resources to identify and address unique security challenges and further the design of safe, secure, and cost-effective reactors.

2. METHOD FOR CREDIBILITY AND CONSEQUENCE LEVEL RANKING

One objective of this work is to yield a technical reference for reactor developers and relevant stakeholders which may be called upon during the development phase of a plant's design. This reference will feature the identification of credible and realistic threats to the passive decay heat removal systems in advanced nuclear reactor designs. To assign metrics for the credibility and realistic nature, this work has drawn upon analyses conducted by subject matter experts, computational modeling, and experimental testing. A resulting qualitative risk-based ranking will serve as a reference, providing engineering-based design considerations and attributes for risk mitigation.

To bound which threats are relevant for consideration, and qualify a prioritized ranking list, threats are evaluated for their probability / credibility, see Table 1, as well as severity of the consequence, see Table 2. The former metric assesses the likelihood of the event occurring, ranging from Very Low where the threat is for all intents and purposes considered non-existent, to Very High, where the event is highly likely. The latter metric assesses the severity of the consequence should an adversary be successful in executing the identified threat. The ranking tables for credibility and consequence, along with an overall assigned risk, were derived from standard categories and rankings levels published in MIL-STD-882A [5].

Lastly, assumption was made to bound capabilities of the adversary, defined as one or more individuals — either insiders or external to the operating nuclear power plant — who plan and execute an attack. Following standard methods and published guidance for addressing threats [6] assumptions were derived from scenarios where a single individual or small group of accomplices organize to execute a given attack. It was also assumed that the accomplice(s) are acting independently and thus are not under the direction of a larger entity or outside country.

Assignment of a threat to within the categories of Credibility and Consequence is based on a scoring system, which for the purposes of this work's analysis is scored 1 – 5, where 1 is assigned to Very Low or Negligible while 5 is assigned to Very High or Catastrophic. Though ultimately assignment of these threat categories levels is subjective and based on recommendations from the author panel and other subject matter experts, judgement is informed based on engineering analysis, direct experience, and/or phenomena-based consideration. For example, some of the threat scenarios identified have not played out in the physical world to any operating plant, however, there is a deep understanding of the methods necessary to achieve the threat, including specific mechanics, along with knowledge of how a plant will be secured and operated. Furthermore, computer models and analysis provide quantitative information on the consequence to an operating plant should specific systems be disabled or modified.

TABLE 1: CREDIBILITY LEVEL RANKINGS

Level	Probability / Credibility
Very High	The occurrence of the event is assessed to be highly likely. Internal decision makers and/or external law enforcement and intelligence agencies determine the event is credible.
High	The occurrence of the event is assessed to be likely. Internal decision makers and/or external law enforcement and intelligence agencies determine the event is credible.
Medium	The occurrence of the event is assessed to be possible. Internal decision makers and/or external law enforcement and intelligence agencies determine the event is known but is not verified.
Low	The occurrence of the event is assessed to be not likely. Internal decision makers and/or external law enforcement and intelligence agencies determine is within realm of possibility but not likely.
Very Low	The occurrence of the event is assessed to be negligible. Internal decision makers and/or external law enforcement and agencies determine event is non-existent or extremely unlikely.

TABLE 2: CONSEQUENCE LEVEL RANKINGS

Severity	Consequence
Catastrophic	Fatalities, mission shutdown, substantial economic losses, significant environmental damage
Major	Severe injuries, partial mission shutdown, major economic losses, major environmental damage
Moderate	Some injuries, some mission time extended, some economic losses, some environmental impact
Minor	Minor injuries, minor mission time extended, minor economic losses, minor environmental impact
Negligible	Negligible or no injuries, no impact on mission, no economic loss, no environmental impact

3. FAILURE MODE HIERARCHY

Identification of security threats began with establishment of a generic failure hierarchy which establishes high level failure modes of a thermal hydraulic system. The broadest failure mode is one based on a process degradation, which includes modified heat transfer (outside of design basis levels), replacement or alteration of working fluid, flow reversals, or rapid heating or cooling. From the process degradations, the team identified generic failure of the structural boundary, driven by either mechanical or thermal loads, followed by plugging or blockage of flow, and lastly, total component failure. Catered to the design principal and operating modes passive decay heat removal systems, these failure hierarchies are expanded upon and derived into a first element category list. In the following subsections, generic descriptions of these security threats are provided. Note, the authors are deliberately omitting details and references to any specific vendor concept or design.

3.1 Altered material property of coolant.
3.2 Blockages or plugging in flow path.
3.3 Change in physical state of coolant.
3.4 Disabling of active support systems.
3.5 External energy into flow path.
3.6 Flow reversals.
3.7 Foreign materials.
3.8 Modified flow path.
3.9 Reduced inventory capacity.

3.1. Altered material property of coolant

An insider could tamper with decay heat removal systems by adding contaminants into the primary working fluid. For example, this could reduce the heat capacity of the coolant, lessening its ability to absorb heat from the designated heat source. However, in this example, a significant quantity of contaminants would be required to achieve an impactful effect, and the changes in coolant properties would likely be detected by quality monitoring systems within the plant. In other scenarios, such as those relying on energetic chemical reactions, the attack method is relatively simple and quantity of required contaminant material significantly less, but the need for insider access and knowledge of the system reduces the likelihood of a successful attack. However, if successful, the potential consequences could be major. In other examples, displacement of the working fluid could be achieved by availability of external sources of non-coolant fluids. This has the potential to cause flow stagnation and complete impairment of the working fluid operation. However, as with the reduced heat capacity scenario, a significant amount of non-coolant fluid would be necessary and likely to be detected by plant personnel.

3.2. Blockages in flow paths

An adversary could disrupt reactor cooling systems by physically blocking the intake, outlet, or mid-run flow paths via the strategic placement of foreign external objects. A sufficient blockage would impede coolant, preventing the reactor from receiving necessary cooling fluid. While a single blockage is more likely to have only minor consequences, given the redundancy in design of these systems, simultaneous attacks on multiple inlets or outlets could result in moderate disruptions and potential damage. Based on redundancy within reactor design of planned decay heat removal installations, these systems can accommodate single blockages thus poising a low acceptable risk. However, simultaneous attacks on multiple inlets or outlets may elevate the risk to an undesirable level.

3.3. Change in physical state of coolant

An adversary through various means could freeze the working fluid of a decay heat removal system. If successful, the consequences would impair or disable the heat removal function, potentially leading to reactor overheating. On the opposing spectrum, induced accelerated evaporation of the coolant is unlikely given the vast volumes of water coolant in water systems, or high boiling point of liquid metals or salts in non-water systems. The probability of the more likely freezing attack varies depending on the coolant type and melting temperatures, where low probabilities occur with lower melting points, and higher probabilities with higher melting points. Mitigating this threat requires robust physical security around primary piping to deter tampering. Despite generally low likelihood, the potential for moderate consequences results in an overall moderate risk level for this threat.

3.4. Disabled active subsystems

An adversary could attempt to disable the heat removal function by tampering with primary pumps, sabotaging storage tanks, or manipulating sensors, valves, etc. In some cases, this might seem like a significant threat, however many passive decay heat removal systems are inherently designed to transition to natural circulation flow during the loss of forced cooling, ensuring continued heat removal even if the pumps are disabled. While some decay heat removal designs incorporate valves that could be manipulated, these are often designed with failure modes to maintain acceptable operation. Therefore, the impact on reactor safety would be minimal, and the reactor would likely continue to be cooled.

3.5. Energy along flow path

An insider or outside familiar with plant and piping layout could employ high energy devices to rupture structures along a closed flow path. A target could focus on traversing piping to reach more sensitive interior chambers, or directly into less sensitive but more exposed inlet or outlet paths. For the latter, assuming that the damage is limited to the chimney portions of the flow path, these consequences could be moderate. However, effective high energy device placement necessitates proximity to critical internal infrastructure, which would be challenging to reach given intricate duct or piping routes within the reactor interior. Furthermore, open discharge or intake ports accessible from the outside would be closely monitored and/guarded, and any attempts to manoeuvre a remote device would triggering security measures and a swift response, If unrestrained access is available to interior portions, and ruptures occurred in large areas, then normal flow paths would be diverted and the heat removal performance of the system could be significantly compromised.

3.6. Flow reversals

An adversary could target exposed inlet and outlet faces to induce flow reversal. This could be achieved by introduction of external heat sources that would trigger buoyancy driven flow directions opposite of normal flow paths. The likelihood of this attack is low, as it requires a large amount of external heat applied over a long duration, specifically during low flow situations, such as during start-up. Alternatively, pressure boundaries could be exploited by diversion of wind from natural sources or active systems. This exploit could disrupt critical cooling

processes, like manipulating temperatures. Regardless of the method, a successful attack could cause flow reversal leading to degraded heat removal and potential damage to reactor components.

3.7. Introduction of foreign materials

An insider could disrupt a facility's thermal radiation systems by the introduction of dust, steam, or smoke between the vessel and the cooling channels. The resulting cloud acts as an insulator, reducing cooling efficiency. This scenario requires the insider to introduce a sufficient volume of dust/steam/smoke to significantly impact heat transfer. The complexity and risk of detection make this attack highly unlikely. While the introduction of dust/steam/smoke could degrade heat removal through radiation, convective heat transfer would likely continue, ensuring adequate cooling performance. Another attack involves introduction of liquid or solid materials that would displace the nominal coolant, such as expanding foam or materials with low thermal conductivities. The need for insider access, knowledge of system weaknesses, and the ability to smuggle and introduce a large quantity of material undetected makes this scenario low probability.

3.8. Modified flow path

One hypothetical sabotage scenario involves a small plane crashing into a facility's external chimney ducts or air vents. Although the chimney stacks or air vents are likely to protrude beyond containment dome and may be easy targets for large object collision, the likelihood of such an attack is low due to air traffic control and security measures around nuclear facilities. However, redundant systems and safety measures would likely prevent catastrophic consequences, and the risk of radioactive material release is minimal due to the assumed small size of the impact. Mitigating this threat involves strategic placement of air vents away from accessible paths during facility design. Alternatively, interior sabotage threats could disrupt flow by creating a short-circuit within the system. An attack creating a direct pathway between hot and cool legs, significantly reduces the system's ability to remove heat. Internal breaches could also be made which redirect coolant to the ambient environment. For air coolants this is likely to have little to no impact, while the consequence could be severe for water systems with limited inventory. However, water systems are expected to employ designs which features two or more parallel networks, so drainage of inventory from a single network would only moderately degrade performance.

3.9. Reduced inventory capacity

An adversary could target coolant inventory holding tanks, disrupting cooling by causing a leak or gradual drainage. While creating a leak or drainage is conceptually simple, the practical execution is challenging. The piping is typically robust and thick-walled, making it difficult to penetrate. Additionally, a single-point access like an unguarded large dump valve is unlikely to be featured in a typical water coolant design, and leakage would need to occur at the lowest elevation point to be effective. These factors, combined with security measures, make the probability of a successful attack low. Also, the decay heat removal design often includes two parallel networks, so drainage from a single network would only slightly degrade performance. Redundant systems and safety measures would likely prevent catastrophic failure, allowing for timely detection and repair.

4. CONCLUSION

By incorporating these insights, reactor vendors can further enhance the security of their passive safety systems. Specifically, they can strategically reduce or eliminate critical indirect sabotage targets within an adversary’s reach. Ultimately, following this research’s guidelines, reactor vendors can leverage an approach that would contribute to the development of safer and more secure advanced reactor designs. Additionally, the assessment and screening of sabotage pathways—deprioritizing those that lack credibility or do not yield significant consequences—remain equally crucial.

ACKNOWLEDGEMENTS

This work was supported by the U.S. Department of Energy National Nuclear Security Administration Agency, Office of International Nuclear Security (NA-211) and the International Nuclear Security for Advanced. Reactors (INSTAR) Program.

REFERENCES

[1] BURGAZZI, L., Addressing the uncertainties related to passive system reliability, Progress in Nuclear Energy 49 (2007).

[2] HIDAYATULLAH, H., SUSYADI, S., SUBKI, M.H., Design and technology development for small modular reactors-Safety expectations, prospects and impediments of their deployment, Progress in Nuclear Energy 79 (2015).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Safety Considerations for Water Cooled Small Modular Reactors Incorporating Lessons Learned from the Fukushima Daiichi Accident, IAEA-TECDOC-1785, IAEA, Vienna (2016)

[4] NUCLEAR ENERGY AGENCY, OECD, NUCLEAR ENERGY AGENCY (Eds), Advanced Nuclear Reactor Safety Issues and Research Needs: Workshop Proceedings, Paris, France, 18 - 20 February 2002, Nuclear safety, OECD, Paris (2002).

[5] MIL-STD-822E: System Safety, U.S. Department of Defense (2012).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).