ENERGY RESILIENCE IN HYBRID-THREAT ENVIRONMENTS: THE ROLE OF SMALL MODULAR REACTORS

DOI: https://doi.org/10.37458/nstf.27.2.3
Original scientific paper
Received: September 9, 2026
Accepted: October 28, 2026

Yordan Katsarov*, Simeon Arnaudov**

Abstract: Hybrid threats - combining cyberattacks, disinformation, sabotage, and conventional disruptions - pose increasing risks to national energy systems. Traditional centralized power generation and long-distance transmission networks are particularly vulnerable to cascading failures under such conditions. This paper

* Assist. Prof. Yordan Katsarov, researcher at the Department of Aviation Equipment and Technologies,Georgi Benkovski Bulgarian Air Force Academy, Dolna Mitropoliya, Bulgaria, yordankatsarov@gmail.com
** Assist. Prof. Simeon Arnaudov, Department of Menigment, Georgi Benkovski Bulgarian Air Force Academy, Dolna Mitropoliya, Bulgaria, simeon.arnaudov@yahoo.com

examines the potential contribution of Small Modular Reactors (SMRs) to strengthening civilian energy resilience in hybrid-threat environments. SMRs offer modularity, distributed siting options, long refueling intervals, and stable low-carbon baseload generation, which together can reduce dependence on single large assets and vulnerable fuel supply chains. The study evaluates how SMR deployment, when integrated with hardened substations, microgrid -capable critical infrastructure, and diversified energy portfolios, can enhance continuity of essential services during multi-vector disruptions. Using a Monte Carlo - based resilience assessment framework, the paper analyzes uncertainty in outage scenarios, restoration times, and common-cause failures to quantify the resilience benefits of SMR networks compared to conventional configurations. The findings suggest that SMRs can significantly improve energy system robustness and recovery capacity - particularly for hospitals, water systems, telecommunications, and emergency operations - provided that sitting, cybersecurity, and auxiliary infrastructure are designed with independence and redundancy in mind. The paper concludes with policy recommendations for integrating SMRs into national resilience strategies while ensuring safety, interoperability, and public trust.

Keywords: hybrid threats, energy resilience, small modular reactors, critical infrastructure, Monte Carlo assessment.

Introduction

Modern energy systems face increasingly complex hybrid threats that blend cyber intrusions, physical sabotage, and information manipulation into coordinated

campaigns capable of disrupting essential services[1,2]. Because electricity supports critical societal functions - from emergency response to digital administration - any prolonged disruption can rapidly escalate into broader systemic instability. Recent incidents across Europe and North America illustrate how adversaries exploit interdependencies within the energy sector to amplify outages and hinder recovery efforts. These evolving risks highlight the limitations of conventional, highly centralized energy architectures, which depend on long transmission corridors and single-point assets that are difficult to protect during multi-vector disruptions. As states seek more resilient and autonomous energy solutions, Small Modular Reactors have gained attention for their potential to support protected microgrids and ensure continuity of critical loads during crises[3].

This paper evaluates the resilience contribution of SMRs under hybrid-threat conditions using a Monte Carlo–based probabilistic framework. The analysis compares a traditional centralized grid with a distributed architecture supported by SMR-anchored microgrids, focusing on outage likelihood, failure propagation, and continuity of essential services. The results demonstrate that SMRs can substantially enhance the stability of critical infrastructure when integrated into hardened, cyber-secure, and independently operable energy nodes. The paper concludes with policy recommendations for incorporating SMRs into national resilience strategies.

[1] NATO CCDCOE, 2023
[2] EU Hybrid CoE, 2024
[3] IAEA, 2022

Background and Literature Review

Hybrid Threats and the Vulnerability of Energy Systems

Hybrid threats combine cyberattacks, disinformation, sabotage, espionage, and conventional pressure into coordinated campaigns designed to destabilize critical infrastructure[4]. Unlike traditional single-vector attacks, hybrid operations exploit systemic interdependencies - particularly in energy systems where digital control, physical assets, and public trust intersect. Research shows that adversaries increasingly target electricity networks to create strategic leverage, disrupt civilian life, and undermine democratic institutions [5].

Historical incidents illustrate the severity of these risks. The 2015-2016 cyberattacks on the Ukrainian power grid demonstrated how coordinated intrusions into "Supervisory Control and Data Acquisition" (SCADA) systems can disable substations and cause widespread outages[6]. The Colonial Pipeline ransomware attack highlighted the vulnerability of energy logistics to cyber extortion [7]. More recently, sabotage of gas infrastructure in Europe underscored the susceptibility of energy networks to physical disruption during geopolitical crises. Energy systems are attractive targets because they serve as foundational infrastructure for all other sectors. Cyber intrusions can manipulate protective relays, disrupt grid balancing, or compromise operator situational awareness. Physical attacks on transformers, pipelines, or transmission towers can produce

[4] DHS, 2022
[5] ENISA, 2023
[6] Lee et al., 2016
[7] CISA, 2021

long-duration outages that overwhelm repair capacity. Disinformation campaigns further complicate response efforts by eroding public confidence in operators and amplifying panic. Together, these dynamics create a complex threat environment requiring new approaches to resilience[8].

Concepts of Energy Resilience

Energy resilience refers to the ability of an energy system to anticipate, withstand, adapt to, and rapidly recover from disruptive events. Contemporary resilience frameworks emphasize four core dimensions: **robustness** - inherent strength of infrastructure to resist disruption; **redundancy** - availability of alternative pathways, generation sources, and operational modes; **resourcefulness** - capacity to mobilize technical, human, and organizational resources during crises; **rapidity** - speed of recovery and restoration of essential services. Traditional mitigation strategies - such as hardening substations, enhancing cybersecurity, and improving emergency response coordination - have improved resilience but remain insufficient against multi vector hybrid threats. Centralized generation architectures, in particular, lack redundancy and are prone to common cause failures. As a result, resilience research increasingly focuses on distributed energy resources, microgrids, and modular generation technologies capable of maintaining critical loads during prolonged disruptions[9].

[8] Chiu, B. et al.
[9] Дамянов, 2023

CC BY NC ND

SMRs in the Evolving Energy Landscape

Small Modular Reactors have gained international attention as potential contributors to resilient, low carbon energy systems. SMRs are characterized by reduced physical footprints, modular construction, passive safety systems, and long refueling intervals, features that differentiate them from conventional large reactors. Their ability to operate in island mode, integrate with microgrids, and provide stable baseload makes them attractive for critical infrastructure protection.

Technical literature highlights several SMR attributes relevant to hybrid threat resilience: -modularity and distributed sitting reduce reliance on single large assets and limit the impact of localized attacks; -passive and inherent safety reduces dependence on external power and active cooling systems, enhancing survivability during cyber physical disruptions; -long refueling cycles minimize exposure to vulnerable supply chains and logistical chokepoints; -compatibility with hardened microgrids enables SMRs to anchor protected energy systems for hospitals, water systems, telecom hubs, and emergency operations centers . Policy analysis from the European Council on Foreign Relations and national energy security agencies argue that SMRs could strengthen European resilience by reducing dependence on imported fuels, mitigating exposure to geopolitical energy coercion, and providing secure power for critical infrastructure[10].

[10] ECFR, 2023

Prior Research on SMRs and Resilience Modeling

Existing studies on SMR resilience primarily focus on technical feasibility, microgrid integration, and operational reliability. Research on nuclear microreactors for defense installations demonstrates how modular reactors can sustain critical missions during grid outages or cyberattacks. Several modeling approaches - such as probabilistic risk assessment, agent-based simulation, and Monte Carlo analysis - have been applied to quantify resilience under uncertain threat conditions. Monte Carlo based resilience modeling is particularly relevant for hybrid threat environments because it allows analysts to incorporate stochastic outage scenarios, variable restoration times, and correlated failures. Prior work shows that Monte Carlo methods can capture nonlinear propagation of failures across interconnected networks, making them suitable for evaluating distributed SMR architectures.

Despite growing interest, literature still lacks comprehensive assessments of SMR networks under hybrid threat conditions that combine cyber, physical, and informational disruptions. This gap motivates the present study, which integrates SMR characteristics into a probabilistic resilience framework to evaluate their potential contribution to national energy security[11].

[11] DOE, 2023

Hybrid-Threat Vulnerabilities in Conventional Energy Systems

Centralized Generation Risks

Conventional energy systems rely heavily on large, centralized generation units - coal plants, gas turbines, and gigawatt scale nuclear reactors - connected through long distance transmission corridors. While efficient under stable conditions, this architecture creates single points of failure that adversaries can exploit during hybrid operations. A successful attack on a major generation node or a critical transmission corridor can trigger widespread outages, overwhelming restoration capacity and causing cascading failures across dependent sectors. Hybrid adversaries have repeatedly demonstrated interest in targeting centralized assets. Physical sabotage of transformers and substations has increased in Europe and North America, while cyber intrusions into large plant control systems have revealed vulnerabilities in legacy industrial control systems. Centralized plants also depend on complex supply chains - fuel deliveries, cooling water access, and external grid support - that can be disrupted through cyber physical or informational attacks. These dependencies reduce operational independence and increase exposure to multi vector disruptions[12].

Cyber Physical Vulnerabilities

Modern power systems rely on digitally integrated control architectures, including SCADA systems, protective relays, automated dispatch tools, and remote monitoring platforms. This digitalization improves

[12] ENTSO E, 2022

efficiency but expands the attack surface available to hybrid adversaries. Cyberattacks can manipulate sensor data, disable protective mechanisms, or cause operators to lose situational awareness - potentially leading to unsafe operating conditions or forced shutdowns. The Ukrainian grid attacks demonstrated how coordinated cyber intrusions can remotely open breakers, disable operator consoles, and corrupt firmware in protective devices. Similar vulnerabilities exist in many European transmission operators, where legacy systems coexist with modern digital platforms. Cyber physical attacks can also be synchronized with disinformation campaigns that sow confusion among the public and emergency responders, amplifying the operational impact of technical disruptions.

Furthermore, interdependence between the power grid and other critical sectors - telecommunications, water systems, transportation - creates cross sector vulnerabilities. A cyberattack on telecom networks can delay grid restoration; a water system outage can compromise cooling for thermal plants; a transportation disruption can hinder fuel delivery. These interdependencies increase the likelihood of cascading failures during hybrid operations[13].

Cascading Failure Mechanisms

Cascading failures occur when an initial disruption propagates through interconnected components, causing sequential outages that exceed system recovery capacity. In centralized grids, high voltage transmission lines,

[13] Alban, A., et al.

substations, and large generators form tightly coupled networks where failures can spread rapidly. Hybrid threats exploit this coupling by targeting nodes whose loss triggers disproportionate downstream effects. Hybrid disruptions often combine simultaneous or correlated failures, such as cyberattacks on control systems paired with physical sabotage of substations or misinformation campaigns that delay operator response. These multi vector attacks increase the probability of common cause failures, events where multiple components fail due to a shared underlying cause. Common cause failures are particularly dangerous because they undermine redundancy and overwhelm contingency plans.

Modelling studies show that centralized grids exhibit nonlinear failure propagation, where small disruptions can escalate into large scale outages depending on network topology, load conditions, and operator response time. During hybrid operations, adversaries may intentionally time attacks to coincide with peak load periods or extreme weather events, further increasing the likelihood of cascading failures. These vulnerabilities highlight the need for distributed, modular, and independently operable energy assets, such as Small Modular Reactors integrated into microgrids, to reduce the risk of cascading failures and enhance continuity of critical services during hybrid threat scenarios[14].

[14] Saket, R. K., & Sanjeevikumar, P.

SMRs as Resilience Assets

Distributed Siting and Network Architecture

Small Modular Reactors offer a fundamentally different architectural model compared to conventional gigawatt scale nuclear plants. Their compact size and modular construction enable distributed siting, allowing multiple reactors to be deployed across a region rather than concentrated at a single location. Distributed SMR networks reduce reliance on long distance transmission corridors, assets frequently targeted in hybrid operations, and limit the impact of localized disruptions. Research on distributed nuclear microgrids shows that geographically dispersed SMRs can maintain critical loads even when parts of the transmission network are compromised. This architecture also reduces common cause failure risk, since the loss of one SMR does not jeopardize the entire system. Distributed siting aligns with modern resilience principles emphasizing redundancy, independence, and modularity [15].

Operational Characteristics Relevant to Hybrid Threats

SMRs possess several operational features that enhance resilience under hybrid threat conditions:

- Passive and Inherent Safety. Many SMR designs incorporate passive safety systems that rely on natural circulation, gravity fed cooling, and simplified reactor geometries. These features reduce dependence on external power, active cooling pumps, and complex operator interventions. During cyber physical

[15] NIST, 2021

CC BY NC ND

disruptions, when external power or control systems may be compromised, passive safety significantly improves survivability.

- Long Refuelling Intervals. SMRs typically require refuelling every 3-10 years, depending on design. This minimizes exposure to vulnerable fuel supply chains, transportation routes, and logistical chokepoints that adversaries may target during hybrid operations.
- High Availability and Stable Baseload Output. SMRs provide stable, dispatchable baseload generation with high-capacity factors comparable to large reactors. This stability is critical for supporting essential services - hospitals, water treatment plants, telecom hubs - during prolonged disruptions when intermittent renewables may be insufficient.
- Microgrid Compatibility. SMRs can operate in islanded mode and integrate with hardened microgrids designed to maintain critical loads independently of the main grid. Microgrid capable SMRs allow critical infrastructure to remain operational even if transmission networks are compromised by cyberattacks or physical sabotage [16].

Integration with Hardened Infrastructure

SMRs can be paired with hardened substations, protected switchyards, and cyber secure digital control systems to create robust energy nodes capable of withstanding hybrid threats. Hardened installations

[16] INL, 2023

typically include reinforced physical barriers, electromagnetic pulse (EMP) protection, redundant communication channels, secure digital instrumentation and control systems. SMRs' smaller footprint and modular design simplify the construction of such hardened facilities compared to large nuclear plants. Their reduced cooling requirements and simplified balance of plant systems also lower the number of critical external dependencies that adversaries could target.

Cybersecurity is a central component of SMR resilience. Modern SMR designs incorporate advanced digital control systems with built in cybersecurity features, including secure architectures, intrusion detection, and segmented networks. These measures reduce the likelihood that cyberattacks can manipulate reactor operations or compromise safety systems[17].

Critical Infrastructure Applications

SMRs are particularly well suited to powering critical infrastructure that must remain operational during hybrid threat disruptions. Studies on nuclear microreactors for defence installations demonstrate that SMRs can sustain mission critical operations during grid outages, cyberattacks, or physical sabotage. Similar benefits apply to civilian infrastructure: hospitals - require uninterrupted power for life support systems, surgical facilities, and digital medical records. SMRs can anchor hospital microgrids, ensuring continuity even during prolonged outages; water Treatment and

[17] DoD, 2022

Pumping Stations - water systems depend on continuous electricity for filtration, disinfection, and pumping. SMRs provide stable baseload power that prevents contamination risks during disruptions; telecommunications - telecom networks rely on distributed nodes that must remain powered to maintain emergency communication. SMRs can support hardened telecom hubs resistant to cyber physical attacks; emergency operations centres - emergency response facilities require secure, independent power sources to coordinate crisis management. SMRs' islanding capability and long refuelling intervals make them ideal for such applications.

Collectively, these applications demonstrate how SMRs can enhance national resilience by ensuring continuity of essential services during hybrid threat scenarios.

Methodology: Monte Carlo-Based Resilience Assessment

Modelling Framework

To evaluate the resilience contribution of Small Modular Reactors (SMRs) under hybrid threat conditions, a Monte Carlo-based probabilistic simulation framework was developed. The framework was designed to compare the resilience performance of two alternative power-system architectures: (i) a conventional centralized grid and (ii) a distributed SMR-based architecture. A total of **10,000 independent simulation runs** were performed. In each realization, disruption events were generated stochastically according to predefined failure probabilities. The same disruption scenarios, probability distributions, and recovery assumptions were applied to both architectures to ensure

a consistent basis for comparison. The analysis focused on the ability of each architecture to maintain electricity supply to critical infrastructure, including hospitals, water-treatment facilities, telecommunications hubs, and emergency-response centers. The primary objective was to quantify differences in system resilience and service continuity rather than to perform a detailed assessment of physical security, cybersecurity, safeguards implementation, or facility protection costs.

The system boundaries include:

- generation assets;
- transmission and distribution infrastructure;
- critical infrastructure loads;
- restoration capabilities;
- operational network configurations.

To ensure a consistent basis for comparison, both architectures were exposed to identical disruption scenarios, threat assumptions, failure probabilities, and restoration characteristics. It should be noted that the objective of the present study was not to isolate the contribution of SMR technology alone, but rather to evaluate the resilience performance of an integrated distributed SMR-based architecture. Consequently, the reported resilience improvements reflect the combined effects of local generation capability, geographical decentralization, microgrid islanding, and system redundancy in addition to the characteristics of SMR technology itself. The results should therefore be interpreted as system-level resilience benefits of the proposed architecture rather than benefits attributable exclusively to SMRs.

Input Variables and Assumptions

The Monte Carlo model incorporates probabilistic input variables representing uncertainties associated with disruptive events and system recovery processes.
The principal input parameters include:

- component outage probabilities;
- transmission and distribution network failure probabilities;
- critical-load demand profiles;
- restoration-time distributions;
- common-cause failure probabilities;
- generation availability factors.

For the distributed architecture, additional parameters describing local generation availability and islanded operation capability were included. These parameters enable the model to represent the ability of distributed generation resources to continue supplying critical loads during wider system disturbances.

To ensure comparability, identical threat assumptions, disruption frequencies, and restoration policies were applied to both architectures. The principal difference between the simulated systems was the architectural configuration of generation resources and their capability to maintain local supply during network disruptions[18]. A summary of the adopted model parameters and assumptions is provided in Table 1. in the appendix.

[18] Hybrid CoE, 2024

Simulation Procedure

The Monte Carlo simulation procedure consists of four sequential steps:

Step 1. Scenario Generation

A disruption scenario is generated through random sampling from the specified probability distributions. Each scenario may affect generation assets, transmission infrastructure, distribution systems, or combinations thereof.

Step 2. System-State Evaluation

The operational status of system components is evaluated following the sampled disruption event. Component availability and network connectivity are determined for the corresponding realization.

Step 3. Critical-Load Assessment

The model evaluates whether designated critical loads remain supplied. A simulation outcome is classified as a critical-load failure whenever one or more critical facilities become unable to receive electrical power.

Step 4. Recovery Simulation and Indicator Calculation

System restoration is simulated using the corresponding recovery assumptions, and resilience indicators are recorded.

The principal indicators evaluated in this study are:

- Critical Load Failure Probability (CLFP);
- Critical Load Continuity Probability (CLCP);
- Expected Outage Duration (EOD);
- Recovery Time Distribution (RTD).

Final indicator values are obtained by aggregating the results from all 10,000 simulation realizations[19].

[19] Ma, R., et al.
[20] WNA, 2022

CC BY NC ND

5.4 Validation, Sensitivity Analysis and Limitations

Model verification was performed by confirming the consistency of simulation outputs with expected power-system behavior under equivalent disruption conditions. In addition, convergence testing demonstrated that 10,000 Monte Carlo realizations provided stable estimates of the selected resilience metrics.

Sensitivity analyses were conducted to evaluate the influence of key model parameters, including:

- generation availability;
- restoration times;
- common-cause failure probabilities;
- distributed generation penetration levels;
- critical-load demand assumptions.

It should be emphasized that the present framework evaluates resilience from the perspective of service continuity and outage performance. The model does not explicitly quantify physical security requirements, cybersecurity costs, safeguards implementation, emergency-planning expenditures, attack-surface expansion, or other security-related consequences associated with the deployment of multiple geographically distributed nuclear facilities. Consequently, the reported results should be interpreted as resilience benefits of the proposed distributed architecture rather than as a complete assessment of all technical, economic, and security implications. These aspects are identified as important areas for future research[20].

Results

The Monte Carlo model was run for 10 000 hybrid threat scenarios involving cyber intrusions, physical sabotage, combined operations, and common cause failures. Each scenario sampled outage probabilities, restoration times, and failure propagation dynamics using the distributions defined in Sec. 5. System performance was evaluated for two architectures: a conventional centralized grid and a distributed configuration supported by Small Modular Reactors.

The conventional grid architecture exhibited a critical load failure probability of **0.864**, indicating that essential services, including hospitals, water treatment facilities, telecommunications hubs, and emergency operations centers, experienced power loss in **86.4%** of the simulated disruption scenarios. This result highlights the vulnerability of centralized power systems to correlated failures, cascading outages, and prolonged restoration times under hybrid threat conditions.

In contrast, the SMR-enhanced distributed architecture demonstrated a critical load failure probability of **0.085**, indicating that essential services remained operational in **91.5%** of the simulated scenarios. This substantially lower failure rate can be attributed to the architecture's ability to isolate critical loads, reduce dependence on long-distance transmission infrastructure, and mitigate common-cause failures through distributed power generation.

The relative reduction in failure probability is given by:

$$\frac{0.864 - 0.085}{0.864} = 0.9016$$

CC BY NC ND

corresponding to a **90.16% reduction in critical load failure probability** relative to the conventional grid architecture. These findings demonstrate that the deployment of distributed SMRs can substantially enhance power system resilience by reducing outage likelihood, limiting failure propagation, and improving the continuity of critical infrastructure services during complex hybrid threat scenarios.

Discussion

The results demonstrate that SMR enhanced distributed architectures offer a substantial resilience advantage over conventional centralized grids when exposed to hybrid threats. The high failure probability observed in the centralized system reflects structural vulnerabilities inherent to long distance transmission corridors, tightly coupled network topology, and restoration processes that are easily disrupted by coordinated cyber physical operations. Under such conditions, even localized attacks can escalate into widespread outages that compromise critical infrastructure.

The SMR supported configuration performs markedly better because it alters how disruptions propagate through the energy system. By anchoring protected microgrids, SMRs reduce dependence on external transmission assets and limit the pathways through which failures can spread. Their ability to maintain islanded operation ensures that critical loads remain powered even when the surrounding grid experiences severe instability. Passive safety features further reduce the likelihood that hybrid threats targeting digital control systems will translate into reactor level failures, strengthening operational continuity during crises.

The 90.16% reduction in critical load failure probability indicates that SMRs do more than incrementally improve resilience - they fundamentally reshape system behaviour under stress. Distributed nuclear baseload provides a stable, autonomous power source that is less susceptible to common cause failures and less reliant on vulnerable logistical or cyber dependent support systems. This structural independence is particularly valuable for facilities such as hospitals, emergency operations centres, water treatment plants, and telecommunications hubs, where uninterrupted power is essential for public safety and crisis response.

These findings align with emerging literature on distributed energy resilience and suggest that SMRs could play a very meaningful role in national strategies aimed at countering hybrid threats. However, their effectiveness depends on appropriate siting, cybersecurity integration, and the design of auxiliary systems that preserve independence from the broader grid. Future work should explore how SMRs interact with other distributed resources, how regulatory frameworks can support protected microgrid deployment, and how public trust can be maintained as nuclear technologies assume a more prominent role in resilience planning.

Policy Recommendations

The Monte Carlo results indicate that Small Modular Reactors (SMRs) can substantially enhance the resilience of critical infrastructure under hybrid threat conditions. To translate these findings into effective national security practice, several focused policy measures should be adopted.

CC BY NC ND

Integrate SMRs into National Resilience Planning

Governments should formally recognize SMRs as resilience assets and incorporate them into hybrid threat preparedness plans, critical infrastructure protection frameworks, and emergency response strategies. SMRs should be treated as stability nodes within distributed, hardened energy architectures rather than solely as generation units.

Prioritize Deployment for Critical Infrastructure

SMR anchored microgrids should be prioritized for facilities where power loss would have severe societal consequences - hospitals, water systems, telecommunications hubs, emergency operations centres, and defence installations. These microgrids must support reliable, islanded operation during cyber physical disruptions.

Modernize Regulatory and Security Frameworks

Regulatory systems designed for large reactors must be updated to enable modular and microreactor deployment. Streamlined licensing, standardized siting criteria, and harmonized cybersecurity and physical security requirements are essential to avoid delays and ensure safe operation in distributed environments.

Strengthen Cybersecurity for SMR Digital Systems

Cybersecurity must be treated as a core safety function. SMR operators should implement segmented network architectures, intrusion detection, regular audits, and coordinated threat intelligence sharing across energy, telecommunications, and defence sectors.

Invest in Hardened Microgrid Infrastructure

To maximize resilience, SMRs should be embedded in hardened microgrids with electromagnetic pulse (EMP) resistant substations, redundant communications, protected switchyards, and secure control centres. These measures reduce common cause failure risk and ensure continuity of critical loads.

Enhance Public Communication and Trust

threats often exploit disinformation. Governments should establish clear communication protocols, rapid response information teams, and public education initiatives on energy resilience and SMR safety to maintain trust during crises.

Conclusion

This study examined the resilience benefits of Small Modular Reactors under hybrid threat conditions using a Monte Carlo based probabilistic modelling framework. Hybrid threats - combining cyberattacks, physical sabotage, and disinformation - pose complex challenges to conventional centralized energy systems, which remain highly vulnerable to correlated failures, long restoration times, and cascading disruptions. The simulation results demonstrate that SMRs, when deployed as distributed, microgrid capable assets, can significantly enhance the continuity of critical infrastructure during such adversarial events.

The Monte Carlo analysis revealed a stark contrast between conventional and SMR enhanced architectures. The centralized grid exhibited a critical load failure probability of 0.864, indicating that essential services

CC BY NC ND

would fail in most hybrid threat scenarios. In contrast, the SMR enhanced distributed configuration reduced this failure probability to 0.085, ensuring operational continuity in 91.5% of simulated disruptions. This represents a 90.16% improvement in resilience, driven by SMRs' passive safety systems, long refuelling intervals, reduced dependence on vulnerable transmission corridors, and ability to operate in islanded mode. These findings reinforce the growing consensus in resilience and security literature that modular nuclear technologies can serve as strategic assets for protecting critical infrastructure. SMRs offer a unique combination of reliability, independence, and survivability that aligns with modern hybrid threat realities. Their integration into hardened microgrids provides a pathway for ensuring uninterrupted power to hospitals, water systems, telecommunications hubs, and emergency operations centres during crises.

While the results are promising, further research is needed to refine the modelling approach, incorporate dynamic adversarial behaviour, and evaluate regulatory, economic, and societal factors influencing SMR deployment. Future work should also explore multi sector interdependencies and real-world demonstration projects to validate the resilience benefits observed in simulation. Overall, this study concludes that SMRs represent a credible, quantitatively supported, and strategically valuable option for enhancing energy resilience. Their deployment within distributed, cyber secure, and hardened energy architectures can significantly reduce the vulnerability of critical infrastructure to hybrid threats and strengthen societal

stability in an increasingly contested security environment.

Literature:

1. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). Cyber-Physical Threats to Energy Infrastructure. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org
2. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). (2024). Hybrid Threats to Energy Infrastructure. Helsinki, Finland: Hybrid CoE. https://www.hybridcoe.fi
3. International Atomic Energy Agency (IAEA). (2022). Advances in Small Modular Reactor Technology Developments: A Supplement to the IAEA Advanced Reactors Information System (ARIS). Vienna, Austria: International Atomic Energy Agency. https://aris.iaea.org/Publications
4. U.S. Department of Homeland Security (DHS). (2022). Critical Infrastructure Threat Analysis Report. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/topics/critical-infrastructure-security
5. European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape for Critical Infrastructure. Heraklion, Greece: ENISA. : https://www.enisa.europa.eu/publications
6. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC: SANS Industrial Control Systems. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf
7. Cybersecurity and Infrastructure Security Agency (CISA). (2021). Industrial Control Systems Cybersecurity Year in Review. Washington, DC: CISA. https://www.cisa.gov
8. Chiu, B., Bose, A., Brown, S., Chalamala, B., Immerman, D., Khodaei, A., Liu, J., Novosel, D., Paaso, A., Rahmatian, F., Romero Agüero, J., & Vaiman, M. (2020). Resilience Framework, Methods, and Metrics for the Electricity Sector (IEEE PES Technical Report PES-TR83). IEEE Power &

Energy Society. DOI: 10.17023/x83h-mn15. https://resourcecenter.ieee-pes.org/publications/technical-reports/pes_tp_tr83_itslc_102920

9. Дамянов, Д. (2023). „Иновативни технологии в поддръжката на самолетите“. В: Годишна университетска научна конференция на НВУ „Васил Левски“, 8-9 юни 2023 г., Велико Търново, България, с. 1223-1230. ISSN 2367-7481.

10. European Council on Foreign Relations (ECFR). (2023). Nuclear Energy and European Strategic Autonomy. London, United Kingdom: ECFR. https://ecfr.eu

11. U.S. Department of Energy (DOE). (2023). Small Modular Reactor Program Overview. Washington, DC: U.S. Department of Energy, Office of Nuclear Energy. https://www.energy.gov/ne/nuclear-reactor-technologies/small-modular-nuclear-reactors

12. European Network of Transmission System Operators for Electricity (ENTSO-E). (2022). Power System Resilience and Restoration Report. Brussels, Belgium: ENTSO-E. https://www.entsoe.eu

13. Alban, A., Darji, H. A., Imamura, A., & Nakayama, M. K. (2017). Efficient Monte Carlo methods for estimating failure probabilities. Reliability Engineering & System Safety, 165, 376-394. Elsevier. DOI: 10.1016/j.ress.2017.03.032.

14. Saket, R. K., & Sanjeevikumar, P. (Eds.). (2024). *Reliability Analysis of Modern Power Systems*. Wiley-IEEE Press. ISBN: 978-1394226740. Available at: Wiley-IEEE Press.

15. National Institute of Standards and Technology (NIST). (2021). Community Resilience Planning Guide for Buildings and Infrastructure Systems. Gaithersburg, MD: National Institute of Standards and Technology. https://www.nist.gov/community-resilience/planning-guide

16. Idaho National Laboratory (INL). (2023). Nuclear Microreactors and Resilient Microgrids. Idaho Falls, ID: Idaho National Laboratory. https://inl.gov

17. U.S. Department of Defense (DoD). (2022). Microreactor Applications for Defense Installations. Washington, DC: U.S. Department of Defense. https://www.defense.gov

18. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). (2024). Hybrid Threats: Multi-Vector Disruption Patterns. Helsinki, Finland: Hybrid CoE. https://www.hybridcoe.fi/all-publications

19. Ma, R., Jin, S., Eftekharnejad, S., Zafarani, R., & Philippe, W. P. J. (2020). A Probabilistic Cascading Failure Model for Dynamic Operating Conditions. IEEE Access, 8, 66444-66458. https://doi.org/10.1109/ACCESS.2020.2984240.

20. World Nuclear Association (WNA). (2022). Small Modular Reactors: Global Status Report. London, United Kingdom: World Nuclear Association. https://world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/small-nuclear-power-reactors

Apendix

Table 1. A summary of the adopted model parameters and assumptions.

Parameter category	Model parameter	Representation in the simulation	Data source or basis	Application to architectures
Simulation settings	Number of Monte Carlo realizations	10,000 independent simulation runs	Selected to obtain stable estimates of the resilience indicators; convergence evidence should be reported	Identical for both architectures
Threat scenarios	Disruption occurrence	Random sampling of disruptive events affecting generation, transmission, distribution, or multiple components	Historical incident data and documented hybrid-threat scenarios; exact sources should be cited	The same sampled scenarios are applied to both architectures
Threat scenarios	Cyber-induced component outage probability	Probability distribution for outages associated with cyber-related disruptions	Historical incident databases or threat assessments; distribution type and parameters to be specified	Identical baseline assumptions for equivalent exposed components
Threat scenarios	Physical disruption probability	Probability distribution for physical damage or loss of component availability	Historical outage records or documented physical incidents; distribution type and parameters to be specified	Identical baseline assumptions for equivalent exposed components
Threat scenarios	Combined disruption probability	Joint or conditional representation of simultaneous cyber and physical disruptions	Assumptions or empirical evidence concerning correlated disruptions; values to be specified	Identical disruption logic for both architectures
Generation	Conventional generation availability	Binary or probabilistic operational state of conventional generation assets	Reliability statistics for conventional generating units; value to be specified	Applied to the conventional architecture
Generation	SMR unit availability	Binary or probabilistic operational state of each SMR unit	Adopted SMR availability assumption; value and supporting source to be specified	Applied to the SMR-based architecture
Generation	SMR capacity	Available electrical output assigned to each SMR unit	Assumed unit rating or selected reference design; value to be specified	Applied to the SMR-based architecture

Parameter category	Model parameter	Representation in the simulation	Data source or basis	Application to architectures
Network	Transmission-line outage probability	Stochastic availability state of each modeled transmission connection	Transmission-system reliability data; distribution and parameters to be specified	Applied consistently to comparable network elements
Network	Distribution-system outage probability	Stochastic availability state of distribution components supplying critical loads	Distribution-system reliability data; distribution and parameters to be specified	Applied consistently to comparable network elements
Common-cause failures	Correlated component failure probability	Joint failure event affecting multiple components during the same realization	Reliability studies or explicitly stated modelling assumptions; value to be specified	Included in both architectures under equivalent disruption conditions
Distributed operation	Islanding capability	Binary operational rule determining whether local generation can continue supplying critical loads following disconnection from the wider grid	Architectural assumption supported by the proposed microgrid configuration	Enabled only where the architecture possesses a technically defined islanding capability
Critical loads	Critical-load demand	Load profile or fixed demand assigned to hospitals, water-treatment facilities, telecommunications hubs, and emergency operations centers	Standardized or case-specific critical-infrastructure demand data; values and sources to be specified	Identical critical-load demand in both architectures
Restoration	Component restoration time	Random variable sampled from an assigned restoration-time distribution	Historical restoration records; distribution type and parameters to be specified	Equivalent component categories use the same restoration assumptions
Restoration	Restoration-resource availability	Parameter representing the availability of repair personnel and required resources	Adopted operational assumption or historical evidence; value to be specified	Identical unless an architecture-specific difference is explicitly justified
Performance assessment	Critical-load failure criterion	A failure is recorded when one or more designated critical loads cannot be supplied during a simulated scenario	Definition adopted in the present study	Identical failure criterion for both architectures

Parameter category	Model parameter	Representation in the simulation	Data source or basis	Application to architectures
Performance assessment	Critical Load Failure Probability	Number of runs containing critical-load failure divided by the total number of runs	Calculated from the 10,000 simulation outputs	Calculated separately for each architecture
Performance assessment	Critical Load Continuity Probability	$1 - P_{\text{failure}}$	Calculated from the simulation outputs	Calculated separately for each architecture
Performance assessment	Expected Outage Duration	Mean duration for which affected critical loads remain unsupplied	Calculated from simulated outage and restoration trajectories	Calculated separately for each architecture
Performance assessment	Recovery Time Distribution	Distribution of the simulated times required to restore critical-load supply	Calculated from restoration outcomes across all runs	Calculated separately for each architecture
Comparison	Relative reduction in failure probability	$(P_{\text{conv}} - P_{\text{SMR}})/P_{\text{conv}}$	Calculated from the estimated failure probabilities	Comparison between the two architectures
Model scope	Security and safeguards consequences	Not explicitly quantified	Physical-protection costs, cybersecurity expenditures, safeguards requirements, emergency-planning costs, and expansion of the attack surface are outside the present model	Recognized as a study limitation