# Development of a Robust Framework for

# Security Assessment of Safety-Informed

# Siting Decisions under Uncertainty

A.I. ADENIYI

Nuclear Energy and Fuel Cycle Division, Oak Ridge National Laboratory, Oak Ridge, TN

Energy Science and Engineering, Bredesen Center, University of Tennessee, Knoxville, TN

U.S.A

Email: [*adeniyiai@ornl.gov*](mailto:adeniyiai@ornl.gov)

O.A. OMITAOMU, Ph.D.

Computational Sciences and Engineering Division, Oak Ridge National Laboratory

Oak Ridge, TN, U.S.A

**Abstract**

The assessment of security vulnerabilities during the initial phase of locating a nuclear reactor facility involves a process that aims to recognize specific site attributes that could expose the site to potential security risks. Early identification of such features is crucial because they could increase the site’s susceptibility to malicious attacks. Any security incident or event could harm life, the environment, or property. Additionally, certain site characteristics, such as its location and the shortest route from first responders, can impact the response to emergencies at the site. Moreover, features such as slope and extreme weather events could influence the efficacy of implemented measures in reducing security risks at the selected site.

If an issue with a site’s potential risk factor is identified early in a facility’s lifetime, then a more cost-efficient plan can be incorporated into the overall site design. However, after a site is chosen and construction commences, any discovery of natural or artificial features that render the site vulnerable to security threats could lead to construction delays and additional expenses in designing and implementing necessary security measures.

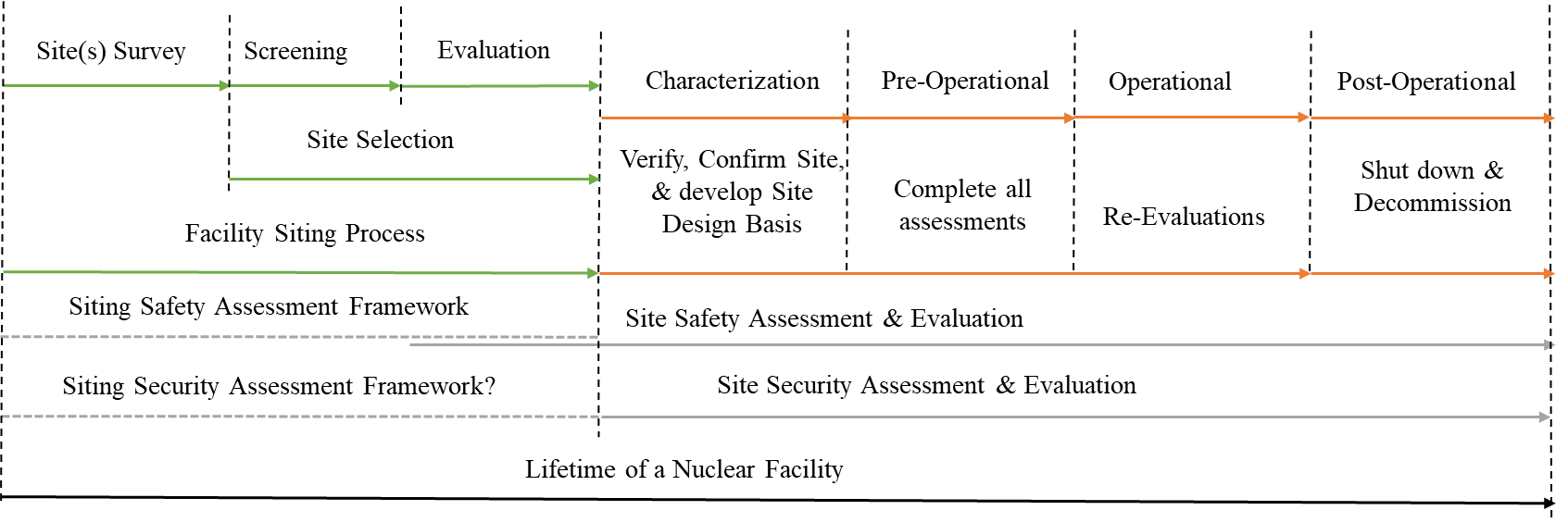
This paper emphasizes the challenges in the evaluation framework used to assess security risks at potential nuclear reactor sites during the site selection phase. Our research underscores the necessity of establishing a robust framework to assess security vulnerabilities in nuclear facility siting and aims to address these gaps effectively.

## INTRODUCTION

Combating challenges posed by climate change, such as more frequent destructive wildfires and floods across the globe, will require implementing innovative energy strategies, including improving energy efficiency, and deploying renewable energy sources and low-carbon footprint energy sources (e.g., nuclear energy). This global decarbonization effort has led to a rise in the acceptance of advanced nuclear reactors as green energy sources. This renewed interest in deploying advanced nuclear reactors—to meet growing demands for electricity, process heat for homes and industrial applications, water desalination, and the potential to deploy nuclear energy for combating some of the challenges of global warming—means there will likely be more nuclear facilities across the globe that may face the constant possibility of security threat (such as sabotage or theft) from malicious attackers.

Evaluating the security vulnerability of a nuclear facility site throughout its operational existence is imperative. The International Atomic Energy Agency (IAEA) delineates three primary actions within the nuclear facility establishment process: a site survey to identify potential sites; the selection process, which involves a comparison of various potential sites based on predetermined criteria pertinent to the particular nuclear technology intended for deployment; and a third phase that entails evaluating a potential site against factors that could jeopardize the facility’s safety or the activities conducted on the premises.

The IAEA emphasized the importance of considering the security of nuclear facilities in the early stages, such as the planning and site selection stages [1]. Early security consideration can result in more effective and better-integrated security, safety, safeguard, and operational measures. The different stages in the lifetime of a nuclear facility are shown in Fig. 1. Safety and security assessments are recommended during all the stages of a nuclear facility’s lifetime by the international and national instruments governing nuclear safety and security. It was recommended in [1] that the impacts of natural and pre-existing site features be assessed along with safety assessment to better integrate safety and security measures. Delaying the assessment of any security vulnerabilities that may be present as a result of site features could result in construction delays and increased costs for implementing security measures, which can sometimes be incompatible with safety and safeguard measures. Delaying could also lead to design modifications during the construction phase. It may be cost-effective to identify site security concerns caused by the features of the site during the siting phase rather than after the site is selected.



*FIG. 1. Site safety and security assessment during the lifetime of a nuclear facility (adapted from [30], [31], [6], and [1])*

## SECURITY VULNERABILITY ASSESSMENT OF THE SITE’S NATURAL AND ARTIFICIAL FEATURES DURING THE SITING PHASE

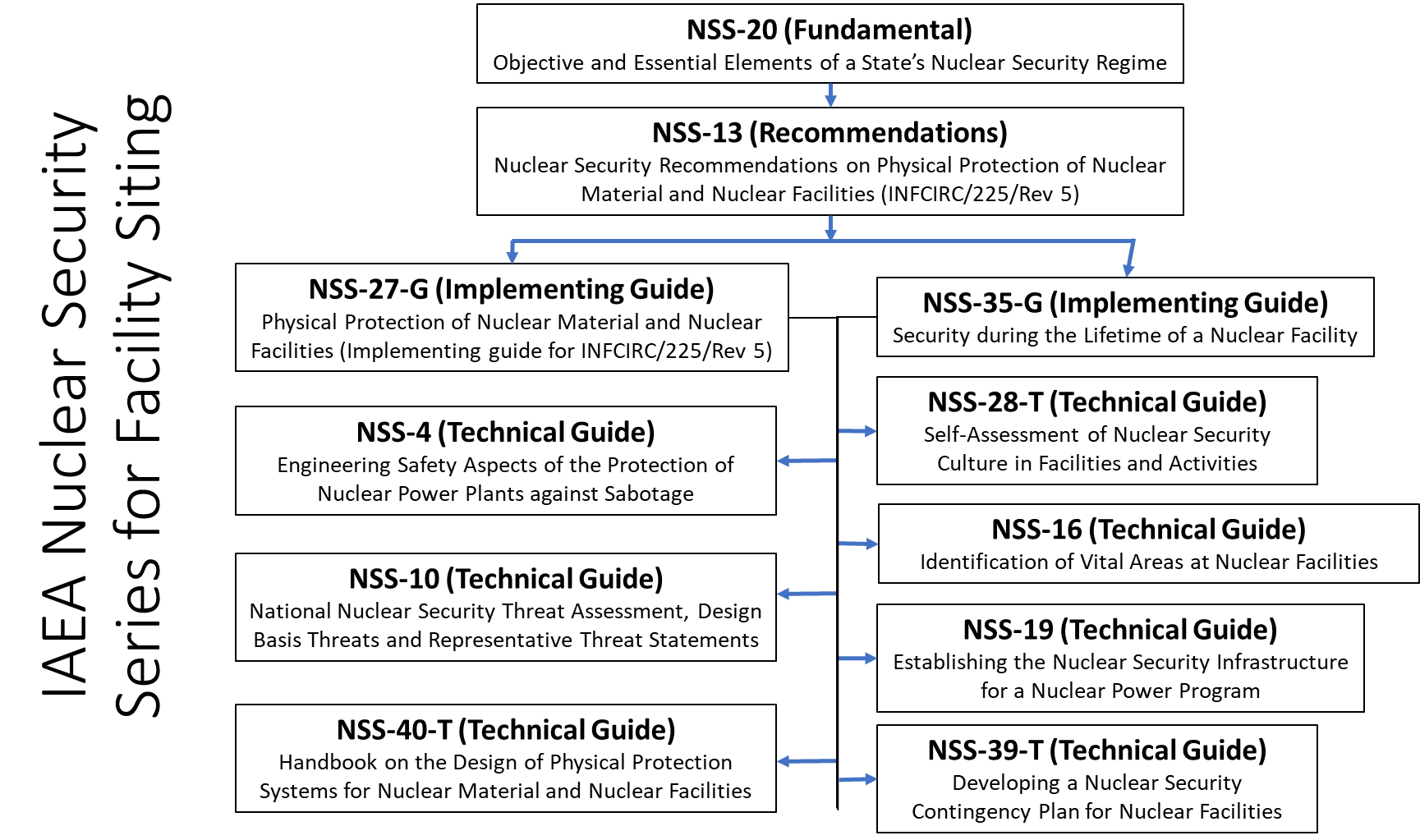
Natural features such as the topology, seismic activity, geology, meteorology, and the area’s hydrology may impact the site’s vulnerability to security threats. Security vulnerability due to features such as mountain ranges, waterways, and local and national borders with neighbors who are politically unstable or are known adversaries should be assessed along with the safety assessment of such features. Other features to consider during the site security vulnerability assessment include the proximity of the site to agencies that will be needed to provide response capabilities to the site in case of a security incident or events; proximity to infrastructure, such as existing hazardous material facilities, existing high-security facilities, airport and air routes, road and rail networks; and the source of the pool of trained personnel required to work at the nuclear facility.

As shown in Fig. 1—which lists some of the safety- and security-related assessments that should be conducted during the lifetime of a nuclear facility—it was not clear, to the best of our knowledge, that a framework exists for assessing a site security vulnerability during the siting phase. This paper examines this as a gap in the site security vulnerability assessment framework during the siting of a potential nuclear reactor facility.

### Gaps in the framework for security vulnerability assessment of nuclear facilities during the siting phase

The nuclear security measures recommended as part of the essential elements of a State’s nuclear security regime in [2], [3], and [4] are focused primarily on security during the operation phase of a nuclear facility. Despite the IAEA recommendation in [1] that “nuclear security considerations should be evaluated alongside safety and other considerations” during the siting process, such security assessments are often delayed past the siting phase; rather, *safety* assessment is often the focus during the siting phase. Site safety assessments, as required by the IAEA in [5], are designed to help ensure the protection of people and the environment from the harmful effects of ionizing radiation. This goal, though important, is different from the nuclear security goal of preventing malicious actors from stealing nuclear material or sabotaging a nuclear facility or nuclear material. The guide [6] developed to assist member States in the implementation of the recommendations provided in [5] does not provide a framework for evaluating a potential site’s security vulnerability; it is suggested in Section 4.8 of the aforementioned document that nuclear security aspects of the site should be considered using the IAEA’s nuclear security series. The concept of a *site*, as used by IAEA in the nuclear security series, usually implies existing nuclear facilities; designations such as *candidate site*, *potential site*, and *selected site* are generally used to represent a green or gray site that is being considered as a new location for a nuclear facility.

A review of the nuclear facility siting-related nuclear security series revealed that there exists guidance in some of the IAEA publications shown in Fig. 2 with respect to on-site security requirements, assessments, and implementation for the lifetime of a nuclear facility; the focus of such instruments was on phases after the siting phase. On the other hand, safety assessment requirements and implementation [5], [6] span all the phases of the nuclear facility’s lifetime.



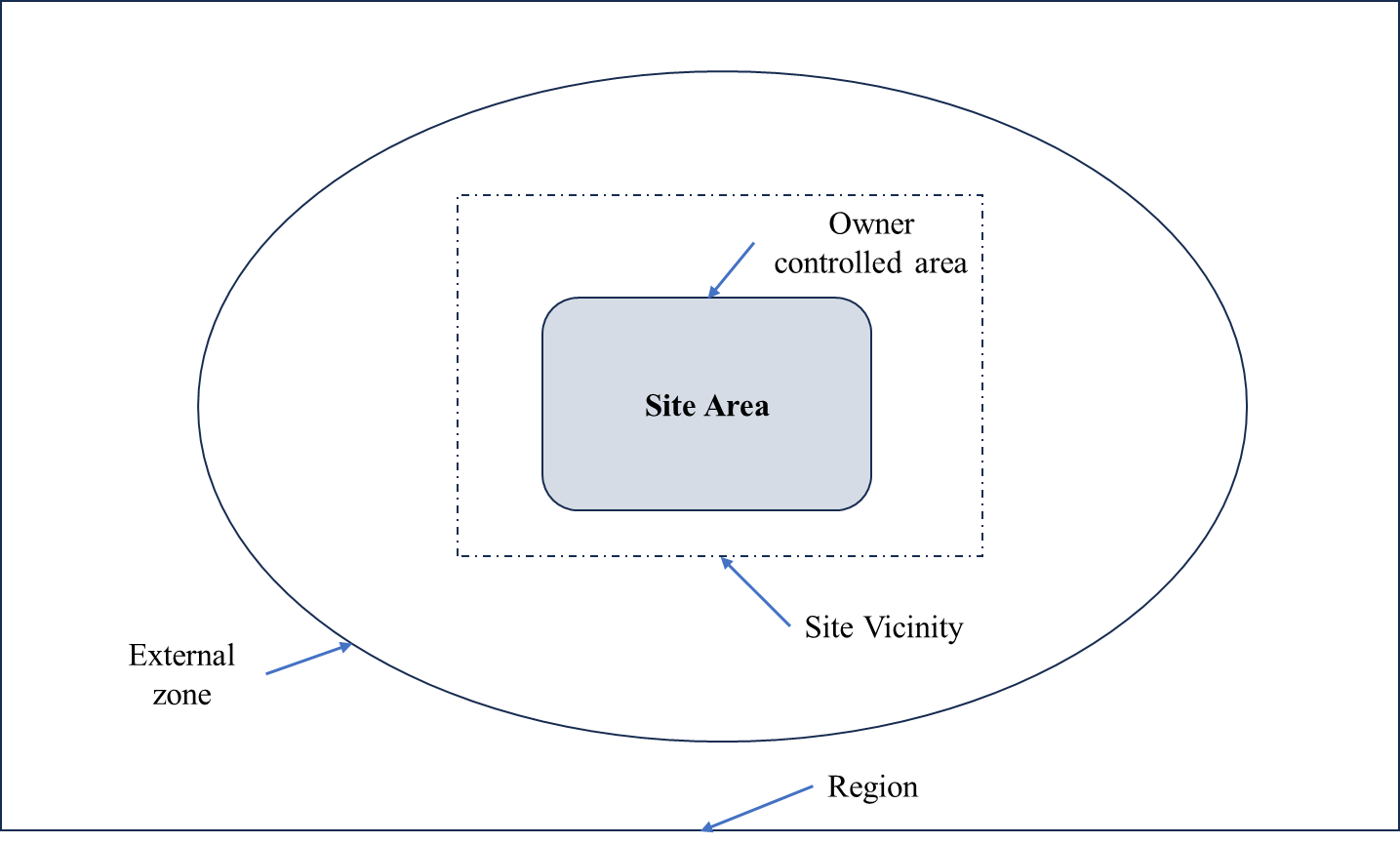
*FIG. 2. Some IAEA Nuclear Security Series relevant to nuclear facility siting (created by the authors).*

In the United States, an applicant for an early site permit for a nuclear facility is required, according to Section 13.6.3 of [7], to provide information demonstrating that adequate security plans and measures can be put in place to address the selected site’s natural and artificial features before an early site permit license can be granted. This NUREG did not specify how such features should be evaluated to determine their security impact.

Nuclear reactor siting activities are governed by legal instruments of the country in which the site is located: for example, in the United States, siting activities are governed by the provisions in regulations such as 10 CFR 100 [8] and Regulatory Guide (R.G.) 4.7 [9]. In 10 CFR 100, the focus of the regulatory requirements is on nuclear safety, which aims to ensure that radiological dose from normal and postulated accidents are acceptably low to people and the environment. This safety-focused goal is different from the nuclear security focus of preventing unauthorized access to nuclear materials and sabotage of nuclear facilities. According to the U.S. Nuclear Regulatory Commission (NRC) in RG 4.7, the suitability of a potential nuclear reactor site is principally determined by the outcome of the site safety consideration, which includes the characterization of the site, site-specific design basis of external events and the examination of emergency management plans, and the environmental considerations; the assessment is focused on the impact of both radiological and non-radiological events on the environment and the public. These site-suitability determining factors are safety-focused, and one could argue that security consideration must be part of the site-suitability determinants. In RG 4.2 [10], Section 9.3.2, the NRC provides a list of reasons why a potential reactor site may not be suitable as a nuclear power site. This list can be used with the provisions in Section 13.6.3 [7] to develop a siting security vulnerability assessment framework.

The NRC has two security assessment–specific guidance documents: NUREG/CR-7145 [11] and NUREG/CR-1345 [12]. In both, the NRC description of facility characterization begins at the plant site’s boundary as defined in the reactor technology power plant’s blueprint. This description does not cover the immediate surroundings of the site boundary, as shown in Fig. 3, and NUREG/CR-1345 recommends that terrain analysis be conducted during the layout design phase; however, this is after the site has been selected. The *site area* contains the plant, defined by a boundary, and is under the effective control of the plant management. Next is the *site vicinity*, which is larger than the site area but smaller than the *external zone*. The *external zone* is the area immediately surrounding a proposed site in which population distribution, density, and land and water uses are considered for their impact on planning effective emergency response actions. The *region* is larger than the *external zone* of the site and is where the site screening for potential candidate sites begins.

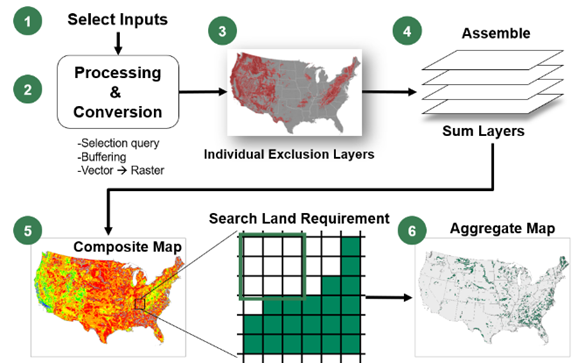
The NRC is undergoing rulemaking to develop alternative physical security requirements for advanced reactors [http://www.regulations.gov/ under docket ID: NRC-2017-0227]. It is yet to be seen whether this proposed NRC guidance will provide a recommendation or require that a site security assessment be conducted in addition to safety assessment during the siting phase.



*FIG. 3. Areas around a nuclear facility site that can impact its suitability (created by the authors).*

The Electric Power Research Institute (EPRI) nuclear reactor site selection guide [13], also known as the *siting guide*, provides expanded guidance, metrics, and criteria that can be used to determine whether a site can support the installation of reactor technology. However, the siting guide focuses on meeting safety and environmental requirements. The siting guide does not address the need to assess the site for security vulnerability for different advanced reactor technologies.

In 2008, Oak Ridge National Laboratory initiated the development of the Oak Ridge Siting Analysis for power Generation Expansion (OR-SAGE) [14]. OR-SAGE is a multi-criteria decision-making framework for siting energy technologies. OR-SAGE uses industry-accepted approaches, national regulations, and energy technology–appropriate selection criteria to screen a region for potential site areas for various power generation technology applications. The OR-SAGE workflow, shown in Fig. 4, has been used to support the development of various power generation technologies [15], [16], and [17]. In its current form, the OR-SAGE framework is facility and environmental safety focused.



*FIG. 4. OR-SAGE’s safety-focused workflow overview (created by the authors).*

In 2013, Idaho National Laboratory developed a site suitability and hazard assessment guide [18] to be used for further site assessment and characterization after a potential site has been identified by a framework like OR-SAGE. This guide, although like the OR-SAGE framework in that it is facility and environmental safety focused, also provides a template in Appendix C-4d for assessing site features that could affect the development of future security measures and adequate security plan as required by 10 CFR 100.21(f) and 10 CFR 73.55. In the template, one of the two site characteristics considered was sufficient site area to support future expansion or deployment of physical protection system (PPS) measures. According to the guide [18], if the distance to any exclusion area at the site is greater than 360 ft (110 m), then the site is considered adequate. The other is that there cannot be public transportation routes that traverse the site.

### Gaps in nuclear facility siting security assessment methodology

The methodologies for developing PPSs for nuclear facility vulnerability risk mitigation strategies should employ a risk-informed approach. This approach should consider the level of each threat as well as the attractiveness and the vulnerability of the targets. It should also consider the potential consequences of the threat if manifested.

International nuclear security instruments recommend that PPSs capable of detecting, delaying, and defeating nuclear threats with high assurance must be put in place to protect nuclear material and nuclear facilities from theft and sabotage by malicious actors. The Convention on the Physical Protection of Nuclear Material (CPPNM) [19] requires that a State’s PPSs should be based on the State’s current evaluation of the threat; thus, a PPS designed for a present threat may not be sufficient to defeat a future threat. Under its fundamental principle G, the amendment to the CPPNM [20] also requires that a nuclear security regime use risk-informed approaches based on a graded approach and defense-in-depth to design PPSs.

In one of the fundamentals listed by IAEA in [2], it is recommended that the State define PPS requirements for nuclear security systems and security measures based on the threat assessment or design basis threat for the physical protection of nuclear materials and nuclear facilities depending on the associated consequences of either unauthorized removal or sabotage. In [3], the IAEA also recommends that the State assess whether the potential threats have the capabilities necessary to cause an unacceptable event for a specific target, facility, or activity. Although a current design basis threat may offer insights into some of the capabilities of a potential threat, it may not provide adequate clues about a future threat’s potential for this reason, new threats are required to be re-evaluated at certain intervals.

Although the goals of safety and security differ, both safety and security vulnerability assessments during the siting phase can be done in a synergic way. This concept of synergic assessment of safety and security is not entirely new, and there are benefits, as alluded to in this paper’s introduction section. Moreover, [21] highlights the importance of the synergy between safety and security during risk assessment, and it also suggests ways to integrate safety and security assessments. Safety assessment frameworks can be used to inform security vulnerability assessment and vice versa, as shown in [22]. It is important to note that there are differences between the two, and they should not be rolled into one concept, as has been done in the past. Baybutt [23] alluded to this possibility by noting that security assessment methodologies were being developed in the past using safety engineering concepts instead of security engineering concepts.

Two main physical security risk assessment methodologies are used to assess the vulnerability of critical infrastructure: the deterministic risk assessment (DRA) approach and the probabilistic risk assessment (PRA) approach. DRA evaluates the impact of a single risk-based factor derived from past incidents and impacts. DRA-based security vulnerability approaches have been developed for critical infrastructure security vulnerability assessments. Table 2 in [24] summarizes such approaches, their areas of application, and their major weakness. The PRA approach allows multiple risk-based factors to be considered to develop various scenarios. PRA-based security vulnerability approaches have been used to assess security vulnerability in critical infrastructure areas such as maritime, chemical plants, pipelines, hazardous material transportation, intruder prevention, and security vulnerability during major events in cities. Examples of specific applications can be found in Tables 3, 4, and 6 in [24].

The PRA methodologies—especially the Bayesian network theory, as used in the chemical process industry [25], [26], [27], [28], and [29]—can be adapted for the vulnerability assessment of critical infrastructure like a nuclear facility during the siting phase. By nature, nuclear security threats are dynamic because the attractiveness of a target as perceived by a malicious attacker can change, so applying the DRA models to assess and quantify nuclear security threats may not yield the optimum result. Another reason the application of the DRA model may not produce the optimum result is that in the DRA model, only the impact of a single risk factor can be evaluated at a time. The risk factor must be based on past incidents or events and their effects. Threats from emergent technologies may not have any of these precursors that can provide meaningful insight into how a malicious attacker can deploy such technologies against a nuclear facility. Continuous improvement in emerging technologies and the unpredictability of the behavior of malicious attackers imply that developing a siting phase security vulnerability assessment methodology based on the PRA is more desirable.

## ADVANCED NUCLEAR REACTORS SITES AND THEIR POTENTIAL SECURITY VULNERABILITIES

Advanced nuclear reactor facilities will be attractive targets for potential malicious actors who may want to steal nuclear materials or sabotage different targets within a facility. Targets within an advanced nuclear reactor site will consist of personnel, equipment, and nuclear material. By design, advanced nuclear reactors will likely have more passive safety-related systems, are sometimes smaller in size than conventional nuclear reactors, and can be built in modules. These advanced design features make them suitable for deployment where conventional nuclear reactors are unacceptable. They can be built closer to population centers, co-located with other energy-generating technologies, or other industries. Some advanced reactor technologies are very small (microreactors < 50 MWt); this size feature makes the microreactor transportable from a fabrication factory to an operator’s site on trucks or by rail. All these unique features of advanced nuclear reactors increase the vulnerability of the nuclear material and the nuclear reactor facility to threats. They may also reduce the effectiveness of some nuclear security measures.

Therefore, locations being considered for advanced nuclear facility siting must be evaluated for nuclear security vulnerabilities, which can inform the development of sufficient threat mitigation measures. Traditionally, nuclear reactor site threat vulnerability evaluation has been performed with a focus on site suitability to provide a safe operating environment for the nuclear reactors. In addition to the assessments of security vulnerability due to the site’s natural and artificial features, the sites to be selected for the deployment of an advanced nuclear reactor must be evaluated for security risks in terms of closeness to the population center and the increased attractiveness for a would-be malicious attacker to cause maximum impact on the nearby population.

## FUTURE WORK

It will be valuable to enhance a framework and assessment methodology to address the siting security vulnerability gaps, such as those in assessment methodology and the apparent lack of clear guidance on evaluating the security impact of natural and artificial features around a nuclear facility site during the siting phase.

Future work will involve applying a Bayesian network–based PRA model coupled with a multi-criteria decision-making risk-informed approach to enhance a framework that can be used to assess a nuclear facility site for security vulnerability during the siting phase. The list of the disqualifying criteria provided in [10] and the provisions in [7] can be used as part of the requirements for developing such a framework.

It will also be prudent to use such a framework to re-assess how the natural and artificial features around existing nuclear facilities can compromise a site’s security in the context of new threats from emerging technologies. This re-assessment exercise can provide insights into how to provide additional mitigation measures against emerging threats.

## Conclusion

The review conducted on existing guidance developed to ensure safe and secure nuclear power operation revealed a gap in the vulnerability assessment framework for addressing security vulnerabilities of potential nuclear facility sites during the early phases of the nuclear reactor facility’s lifetime. Existing guidance is mainly focused on assessing the natural and artificial features of a potential nuclear reactor facility site that can compromise the safety of the reactor and the facility. Developing a vulnerability assessment framework for the siting phase can help identify features that can make the implementation of future security measures challenging and costly. Natural and artificial features of a potential site can make it vulnerable to malicious attacks or impact the effectiveness of physical security measures. For example, emergency responders’ proximity to a site may impact responders’ accessibility to the site in case of security event. Also, a potential site that is surrounded by high elevations may be vulnerable to malicious aerial attacks.

ACKNOWLEDGEMENTS

The work presented in the paper was sponsored by the United State National Nuclear Security Administration’s Office of International Nuclear Security under the Advanced Reactor program. This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The U.S. government retains the publisher, by accepting the article for publication, acknowledges that the U.S. government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (<https://energy.gov/downloads/doe-public-access-plan>).

References

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).
2. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
3. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
4. INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (2016).
6. INTERNATIONAL ATOMIC ENERGY AGENCY, Site Survey and Site Selection for Nuclear Installations, IAEA Safety Standards Series No. SSG-35, IAEA, Vienna (2015).
7. U.S. NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants NRC NUREG-0800, NRC, USA (2016).
8. U.S. Code of Federal Regulations, "Reactor Site Criteria," Part 100, Title 10 "Energy." 10 CFR 100, NRC, USA https://www.nrc.gov/reading-rm/doc-collections/cfr/part100/index.html (page last accessed 10, 2023).
9. U.S. NUCLEAR REGULATORY COMMISSION, General Site Suitability Criteria for Nuclear Power Stations, NRC Regulatory Guide RG 4.7, NRC, USA (2014).
10. U.S. NUCLEAR REGULATORY COMMISSION, Preparation of Environmental Reports for Nuclear Power Stations, NRC Regulatory Guide RG 4.2, NRC, USA (2018).
11. U.S. NUCLEAR REGULATORY COMMISSION, Environmental Standard Review Plan: Standard Review Plans for Environmental Reviews for Nuclear Power Plants, NRC, NUREG/CR-7145, Washington, DC (2013)
12. U.S. NUCLEAR REGULATORY COMMISSION, Nuclear Power Plant Security Assessment Technical Manual, NRC, NUREG/CR-1345, Washington, DC (2013)
13. EPRI 2022, Advanced Nuclear Technology Site Selection and Evaluation Criteria for the New Nuclear Energy Generation Facilities, EPRI, 2022. https://www.epri.com/research/programs/065093/results/3002023910#:~:text=The%20primary%20objectives%20of%20the,economic%2C%20and%20environmental%20justice%20considerations. (Last accessed 10/2023).
14. MAYS, G. T., et. al. (May 2012). Application of Spatial Data Modeling and Geographical Information Systems (GIS) for Identification of Potential Siting Options for Various Electrical Power Generation Sources, ORNL/TM-2011/157/R1. Oak Ridge National Laboratory. <https://info.ornl.gov/sites/publications/files/Pub30613.pdf>
15. MAYS, G. T., et. al. (June 2012). Application of Spatial Data Modeling Systems, Geographical Information Systems (GIS), and Transportation Routing Optimization Methods for Evaluating Integrated Deployment of Interim Spent Fuel Storage Installations and Advanced Nuclear Plants, ORNL/TM-2012/237. Oak Ridge National Laboratory.
16. BELLES, R. J., et. al. (March 2013). Evaluation of Suitability of Selected Set of Coal Plant Sites for Repowering with Small Modular Reactors. ORNL/TM-2013/109. Oak Ridge Nation Laboratory.

<https://info.ornl.gov/sites/publications/files/Pub41833.pdf>

1. BUCKNOR, M., FORD, M. HUMMEL, J., SAMSA, M., BELLES, R., OMITAOMU, O., BAKER, S., and HOELZLE, G. (March 2021). National Demonstration Reactor Siting Study – Phase I, Revision 1. United States. <https://publications.anl.gov/anlpubs/2021/04/167516.pdf>
2. IDAHO NATIONAL LABORATORY, Site Suitability and Hazard Assessment Guide for Small Modular Reactors. INL/EXT-13-29749, October 2013 <https://inldigitallibrary.inl.gov/sites/sti/sti/5806458.pdf>
3. Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980).
4. Amendment to the Convention on the Physical Protection of Nuclear Material GOV/INF/2005/10-GC (49) INF/6, IAEA, Vienna (2005).
5. ROY, N. et. al, 2016. A review of safety indices for process design. Curr. Opin. Chem. Eng. 14, 42–48. <https://doi.org/10.1016/J.COCHE.2016.07.001>.
6. RENIERS, G., et.al, 2020. What safety models and principles can be adapted and used in security science? J. Loss Prev. Process. Ind. 64, 104068 https:// doi.org/10.1016/J.JLP.2020.104068.
7. BAYBUTT, P., 2017. Issues for security risk assessment in the process industries. J. Loss Prev. Process. Ind. 49, 509–518. <https://doi.org/10.1016/J.JLP.2017.05.023>.
8. VARADHARAJAN, S., BAJPAI, S., Chronicles of security risk assessment in process industries: Past, present and future perspectives. Journal of Loss Prevention in the Process Industries. https://linkinghub.elsevier.com/retrieve/pii/S0950423023001262, 2023
9. ARGENTI, F., LANDUCCI, G., RENIERS, G., COZZANI, V., 2018. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab. Eng. Syst. Saf. 169, 515 –530. <https://doi.org/10.1016/J.RESS.2017.09.023>.
10. SONG, G., KHAN, F., YANG, M., 2019. Probabilistic assessment of integrated safety and security related abnormal events: a case of chemical plants. Saf. Sci. 113, 115–125. <https://doi.org/10.1016/j.ssci.2018.11.004>.
11. MISURI, A., KHAKZAD, N., RENIERS, G., COZZANI, V., 2019. A Bayesian network methodology for optimal security management of critical infrastructures. Reliab. Eng. Syst. Saf. 191 <https://doi.org/10.1016/j.ress.2018.03.028>.
12. ZHU, R., HU, X., LI, X., YE, H., JIA, N., 2020. Modeling and risk analysis of chemical terrorist attacks: a bayesian network method. Int. J. Environ. Res. Publ. Health. <https://doi.org/10.3390/ijerph17062051>.
13. GEORGE, P.G., RENJITH, V.R., 2021. Bayesian estimation and consequence modeling of deliberately induced domino effects in process facilities. J. Loss Prev. Process. Ind. 69, 104340 <https://doi.org/10.1016/j.jlp.2020.104340>.
14. INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSR-1, IAEA, Vienna (2019).
15. INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. NSS-19, IAEA, Vienna (2013).