**Transitioning Regulatory Oversight: Moving from Prescriptive to Performance-Based Approach for Addressing Security Challenges in Indian Small Modular Reactors (SMRs)**

KAUSHIK GHOSHAL\*

Kaushikghoshal1986@gmail.com

Nuclear Controls and Planning Wing

Department of Atomic Energy

Government of India

Mumbai; India

ANEK KUMAR

Nuclear Controls and Planning Wing

Department of Atomic Energy

Government of India

Mumbai; India

GARIMA SHARMA

Nuclear Controls and Planning Wing

Department of Atomic Energy

Government of India

Mumbai; India

***Abstract***

The deployment of small modular reactors (SMRs) holds significant promise for India’s energy security and sustainability goals. However, the unique security challenges due to their modularity, potential deployment in urban locations, and evolving design characteristics pose unique security challenges. The existing prescriptive based regulatory requirements (nuclear security), tailored for conventional reactors, might not adequately address these SMR-specific security concerns. Therefore, it is imperative to conduct a thorough evaluation of existing nuclear security requirements to ensure they effectively address these concerns and facilitate compliance. This abstract presents a study aimed at evaluating the adequacy of India’s nuclear security requirements in addressing security challenges associated with SMR deployment and proposes recommendations for enhancing regulatory oversight and compliance. The study employs a mixed-methods approach, combining qualitative analysis of nuclear security requirements documents and guidelines with stakeholder’s expectation and expert consultations. The analysis focuses on key aspects of India’s regulatory requirements, including licensing requirements, security standards, emergency preparedness, and regulatory enforcement mechanisms. Additionally, international best practices are reviewed to benchmark India’s regulatory approach against global standards.

1. ***Introduction:***

The nuclear power sector in India is on the brink of substantial expansion, with small modular reactors (SMRs) emerging as a promising solution to address the nation's escalating energy demands. Preliminary sites for SMRs are being considered at locations such as decommissioned large commercial thermal power plants, where their operational lifespans have ended. Additionally, potential sites include areas within large industrial complexes, like integrated steel plants or aluminium smelters, hosting captive power plants. These captive power plants, essential for meeting significant electricity demands, face operational difficulties due to aging infrastructure, resulting in heightened operational and maintenance costs compounded by escalating fossil fuel prices. However, the deployment of SMRs, particularly within urban landscapes, presents distinct security challenges owing to their potential proximity to densely populated areas. Unlike conventional large-scale reactors, which are typically situated within exclusion zones of at least 1 km [1], SMRs deployed in urban settings may lack such spatial buffers.

However, according to the U.S. Nuclear Regulatory Commission (USNRC), next-generation reactors are anticipated to possess risk characteristics of such low magnitude that the safety of the public is reasonably assured solely by the design and operational parameters of the reactor and plant. This leads to an exceedingly low probability of a severe accident occurring. Such a facility is capable of meeting the Quantitative Health Objectives (QHOs) outlined in the Safety Goal, with exclusion area distances potentially as minimal as 0.1 miles (160 Metres). The consequences of accidents within design parameters, assessed using updated source terms and a pragmatic evaluation of engineered safety features, are likely to be deemed acceptable within distances of 0.25 miles (400 Metres) or less [2].

As SMR technology rapidly progresses towards implementation, it's essential for key stakeholders, including the State Competent Authority, Regulatory Body and Operator, to proactively address nuclear security implications, as emphasized in Section-3 of NSS-13 [3]. This involves considering factors such as the need for additional regulations to accommodate new technologies and adopting a graded approach, ensuring clarity on the division of responsibilities for nuclear security implementation in public/private consortiums, addressing questions about whether security components for SMRs should meet the same rigorous standards as traditional nuclear power plants and the legal aspects of ownership, evaluating concerns about potential sabotage consequences like Unacceptable (URC) or High Radiological Consequences (HRC) based on existing regulations [4].

For upcoming SMRs, there is growing concern about the effectiveness of conventional security protocols, notably the "deterrence, detection, delay, and response" component within the physical protection system (PPS). The absence of the conventional exclusion zone (Presently 1 Km), serving as a vital buffer area, not only prolongs the time required for an unauthorized breach but also directly compromises the efficacy of deterrence, detection, and response protocols. In traditional facilities, the presence of large exclusion zones naturally provides inherent delays, aiding in thwarting unauthorized access. However, with SMRs situated in urban settings, the absence of such expansive buffers necessitates the development of alternative security strategies to address the heightened importance of resilient deterrence, swift detection, and rapid response in safeguarding critical assets.

The prevailing regulatory framework in the India predominantly employs a prescriptive methodology concerning nuclear security, grounded in predefined rules and regulations. While this approach effectively establishes fundamental security standards, its adaptability to the unique security demands of urban SMRs remains questionable. The absence of traditional exclusion zone (1 Km) mandates a more dynamic Nuclear Security framework capable of addressing the specific threats and vulnerabilities inherent in urban SMR deployment.

The present study advocates for a transition from prescriptive to performance-based regulation of security in Indian context. A performance-based approach prioritizes the achievement of predetermined security outcomes over the imposition of specific methodologies. This paradigm shift enables greater flexibility in devising and implementing security measures tailored to the distinctive urban contexts surrounding each SMR. By fostering innovation in security technologies and endorsing a risk-informed approach, a performance-based framework can augment the overall security resilience of Indian SMRs in urban settings, thereby ensuring the safe and secure integration of this promising clean energy technology.

The present study utilizes a mixed-methods methodology, integrating qualitative examination of nuclear security requisites and directives with consultations from stakeholders and experts to gather their perspectives. The examination centres on crucial facets of India's regulatory prerequisites, encompassing licensing criteria, security requirements, emergency readiness, and mechanisms for regulatory enforcement. Furthermore, international practices are scrutinized to assess India's regulatory framework against global norms and practices.

1. ***Security Risks of Small Modular Reactors (SMRs) In Urban Landscapes:***

The deployment of small modular reactors (SMRs) in urban areas presents distinct security challenges. Firstly, their compact size increases the risk of sabotage or theft, as adversaries may find it easier to gain access to vital areas of the reactor facility and its radioactive materials. This vulnerability heightens concerns regarding the potential for unauthorized access and malicious activities. Secondly, the smaller exclusion zone or No Exclusion Zone associated with SMRs amplifies the risk of a radiological release in the event of a successful attack. Such a release could lead to Unacceptable Radiological Consequences (URC) or High Radiological Consequences (HRC), posing a significant threat to public health and safety. The limited buffer zone surrounding urban SMRs exacerbates the potential impact of such incidents on nearby populations and the environment. Additionally, the absence of a substantial exclusion zone reduces the ability of emergency responders to swiftly and effectively address security incidents at SMRs. This limitation may impede the timely deployment of emergency measures and exacerbate the consequences of security breaches, further emphasizing the need for robust security protocols and response strategies tailored to the unique challenges of SMRs in urban settings.

1. ***The Prescriptive Model of Nuclear Security Regulations in India:***

India's current approach to nuclear security regulations follows a prescriptive model. However, to fully understand this model, we must first delve into the physical security measures employed at Indian Nuclear Power Plants (NPPs). These facilities boast a robust system of three concentric boundaries.

The innermost layer is the Operating Island (OI) boundary, typically secured with double fencing. This critical zone encompasses all safety-related systems and structures essential for the plant's safe operation. Key nuclear facilities, systems, and structures such as the reactor, containment building, and emergency systems reside within this boundary. While not safety-related, auxiliary systems located outside this zone may still hold significance in overall plant operations.

The next layer outwards are the Main Plant Boundary (MPB). This boundary encloses the entire nuclear facility, encompassing both safety-related and auxiliary systems and structures essential for safe operation.

Finally, the outermost layer is the Exclusion Zone boundary, which extends up to 1.6 kilometres around the plant. Public habitation is strictly prohibited within this zone. Plant fencing physically isolates this area, and plant management maintains meticulous control over it.

In the present Prescriptive based Security Regulation model, meticulous attention is given to various parameters, including the delineation of distances between Main Plant Boundary (MPB) and ‘OI’ Boundary and heights for these boundaries, the selection of construction materials, provisions for visibility through the walls, establishment of patrolling routes, strategic placement of watchtowers, and specifications for surveillance equipment such as CCTV cameras in terms of positioning, resolution, and type, Security Infrastructure of Central Alarm Stations and Security Control Room etc.

Furthermore, the security protocol encompasses a comprehensive approach to access points, encompassing the Exclusion Zone boundary gate, Main Plant Boundary gate (referred to as Main Guard House), Operating Island gate, and entry portals to Vital Areas. Each of these access points is fortified with stringent credential verification procedures, ensuring that only authorized personnel gain entry to designated areas.

It is essential to underscore that the security architecture is designed to create a robust defence mechanism, requiring individuals to navigate through a series of meticulously monitored checkpoints. This layered approach significantly enhances security measures, effectively deterring potential intrusions and safeguarding the integrity of the facility.

1. ***The Pitfalls of Prescriptive Security Regulation Models:***

The efficacy of Prescriptive Security Regulation Models in ensuring the security of Small Modular Reactors (SMRs) encounters challenges, particularly in urban landscapes where space constraints limit the implementation of traditional security approaches. The prescribed model necessitates extensive areas to accommodate concentric layers of security, a luxury often unavailable in densely populated urban environments. Consequently, maintaining the requisite distances between these layers becomes impractical, affecting the integrity of the security measures. As a result, the layout of SMRs must adapt to the available land, necessitating unique configurations tailored to the specific landscape. This flexibility in layout design, while essential for integrating SMRs into urban settings, poses a significant obstacle to the rigid requirements imposed by Prescriptive Security Regulation Models. Each SMR's layout becomes inherently distinct, reflecting a nuanced approach that prioritizes practicality within the confines of urban land use. Consequently, the uniform implementation of prescriptive security measures across SMRs becomes unfeasible, as each facility's design must contend with the spatial limitations of its surroundings. In essence, the inflexibility of Prescriptive Security Regulation Models proves incompatible with the dynamic nature of SMR deployment in urban landscapes, highlighting the need for adaptable security strategies that can accommodate varying spatial constraints without compromising safety and integrity.

1. ***Adoption of “Security by Design” Approach:***

Based on the current assessment, consensus among stakeholders indicates that embracing the Security by Design philosophy would be appropriate for upcoming Small Modular Reactors (SMRs). This approach entails integrating security considerations into every phase of the design process, ensuring that security measures are intrinsic rather than add-ons. By adopting Security by Design principles, organizations aim to proactively mitigate risks, enhance resilience, and create robust security frameworks that are inherently resilient to threats and vulnerabilities. Delineated below are the fundamental principles of Security by Design [5].

1. ***Holistic Integration:*** Collaborating with engineering and safety experts to create cohesive security systems. This includes the seamless integration of physical and cyber security specialists from the outset of the design phase.
2. ***Inherent Security:*** Incorporating security considerations into the initial stages of designing plants, facilities, buildings, and systems. This proactive approach ensures that security is ingrained into the foundation of the infrastructure.
3. ***Passive Defence:*** Minimizing reliance on active security measures and human intervention to mitigate security risks. Emphasizing passive security measures reduces vulnerability and enhances overall resilience.
4. ***Adaptive Responsiveness:*** Fostering the capacity for agile responses to evolving threat landscapes. This involves maintaining the flexibility to adapt security systems in anticipation of emerging and unforeseen threats.

The following examples illustrate the application of Security by Design principles in mitigating risks and enhancing security:

* ***Mitigation of Malicious Acts:***
* Underground placement of vital areas to mitigate risks from airplane crashes or stand-off attacks, thereby reducing potential radiological consequences in case of sabotage.
* ***Prevention and Response against Threats:***
* Strategic positioning of security posts staffed by armed personnel capable of swift and efficient responses to multiple targets or vital areas.
* Designing fortified positions near vital areas to withstand ballistic and explosives attacks, strategically positioned to counter adversarial threats.
* Implementation of Multi-purpose Central Alarm Stations (CAS) equipped with surveillance and monitoring capabilities for safety, security, and Nuclear Material Accounting and Control (NMAC). CAS serves for daily operation monitoring, security surveillance, and emergency response.
* Establishment of a comprehensive IT Security Management System to ensure proper handling, classification, and management of sensitive and classified information.
1. ***Dynamic Defence: Transitioning to*** ***Performance-Based Security Measures:***

A performance-based approach, which focuses on achieving predetermined security outcomes rather than dictating specific layouts, could be a more suitable alternative for securing urban SMRs. This approach allows for greater flexibility in designing and implementing security measures that are tailored to the specific vulnerabilities and threats posed by the unique urban environment surrounding each SMR. By fostering innovation in security technologies and facilitating a risk-informed approach, a performance-based framework can offer a more adaptable and effective solution for securing SMRs in urban settings [6].

In Performance-Based approach, effective physical protection system (PPS) design for nuclear facilities necessitates a systematic approach. The process begins with a comprehensive security assessment that gathers information about the facility, defines potential threats [Design Basis Threat (DBT)], and identifies critical targets. This assessment informs the design of the PPS, which typically incorporates detection, delay, and response elements. A thorough analysis of the PPS design evaluates each element's effectiveness in achieving the overall physical protection objectives. This analysis ensures that all components contribute proportionately to the overall system's effectiveness.

Balancing security with resource constraints is critical for Plant Management. Evaluating the proposed PPS design involves weighing its effectiveness against available resources. Due to the intricate nature of these systems, computer simulation techniques are often used to assess vulnerabilities and optimize the design. Identified vulnerabilities require redesign and re-evaluation of the system [7].

Finally, a risk assessment is conducted to quantify the overall risk associated with the PPS. This risk is normalized against the potential consequences of a successful attack on a specific target. In simpler terms, the potential consequences of losing an asset are assigned a numerical value between zero and one, with one representing the most severe consequence. This risk ranking enables facility management to make informed decisions about the acceptability of residual risk [8].

1. ***Methodology:***

The effectiveness of PPS (PE) is defined as the product of two probabilities: Probability of Interruption (PI) and Probability of Neutralization (PN). We will use risk (R) to determine the overall system performance.

$R=P\_{A}×[1-P\_{E}]×C$ …………………………………………………………….. (1)

In equation (1) PA is the probability of attack

PE is the physical protection system effectiveness given as

$P\_{E}=[P\_{I}×P\_{N}]$ ……………………………………………………………………… (2)

$[1-P\_{E}]$ is the probability of system failure

C is the consequences of the attack

It is a probabilistic approach which evaluates the PPS functions with respect to Response Force Time (RFT). There are multiple paths that can be followed by the adversary from the offsite area to the target area. Each possible path has different protection layers with several security elements. For each pathway, software can determine the PI value. The detection and delay components of the PPS, along with the respective value of Probability of Detection (PD), mean delay time (tD), and Probability of Communication (PC) are measured along a specific adversary path and are used as inputs in the Adversary Sequence Diagram (ASD). The Response Force Time (RFT) is used to decide the Critical Detection Point (CDP) in the ASD [9].

To achieve a robust level of protection, the Physical Protection System Effectiveness (PE) value should ideally be at least 0.8. This can be attained by ensuring a Probability of Interruption (PI) and a Probability of Neutralization (PN) of at least 0.9 each. This combination would result in a product of 0.81, exceeding the target PE value.

1. ***Key design considerations to address Security Challenges in Dynamic Defence***

To ensure the safe and secure operation of SMRs in such environments, a comprehensive approach to security is essential. This includes the implementation of various remedial measures aimed at mitigating security risks and safeguarding both the reactor facilities and surrounding communities.

1. Enhanced Physical Protection Systems
2. Cybersecurity Safeguards
3. Redundant Safety Systems
4. Continuous Risk Assessment and Adaptation
5. ***Proposed Strategy: Essential Design Factors for tackling Security Challenges in Dynamic Defence***
6. **Enhanced Physical Security Infrastructure: A Closer Look**
7. **Multi-layered Security**
8. **Advanced Surveillance Technologies**
9. **Robotic Security Patrols**
10. **Cybersecurity Integration**
11. **Artificial Intelligence (AI) and Machine Learning (ML) Integration**
12. **Real-time Threat Assessment and Response**
13. **Drone Detection and Countermeasures**
14. **Resilient Physical Infrastructure**
15. **Examining Redundancy in Safety Systems**

Redundant safety systems for small modular reactors (SMRs) play a crucial role in enhancing the overall safety of these nuclear power plants, particularly in urban environments where the absence of large exclusion zones poses unique challenges. While conventional nuclear reactors typically rely on multiple layers of safety systems, SMRs may require additional redundancies due to their smaller size and potential proximity to populated areas.

The goal of redundant safety systems is to provide multiple backup mechanisms to prevent or mitigate the consequences of potential accidents or malfunctions. These systems act as fail-safe measures, ensuring that even if one safety system fails, another can take over and prevent a severe incident.

In the context of SMRs, redundant safety systems can be categorized into two main types:

1. **Inherent Safety Features**
2. **Engineered Safety Systems**

Specific examples of redundant safety systems for SMRs include:

* **Multiple Emergency Shutdown Systems:** SMRs may employ multiple independent emergency shutdown systems to ensure the reactor can be quickly and safely shut down in the event of an abnormal condition. These systems may include control rod insertion systems, emergency boron injection systems, and passive shutdown mechanisms.
* **Diverse Decay Heat Removal Systems:** Redundant decay heat removal systems are essential for removing the residual heat produced by the reactor even after it has been shut down. SMRs may utilize multiple cooling systems, such as natural circulation loops, active water-cooling systems, and air-cooling systems, to provide diverse and reliable decay heat removal capabilities.
* **Multiple Containment Barriers:** SMRs may incorporate multiple containment barriers to prevent the release of radioactive materials into the environment. These barriers may include the reactor vessel, containment building, and additional confinement systems, providing multiple layers of protection against radioactive releases.
* **Redundant Radioactive Material Filtration Systems:** SMRs may employ redundant filtration systems to remove radioactive particles from the air and water pathways before they are released to the environment. These systems may include multiple stages of filtration, such as HEPA filters, charcoal filters, and iodine filters, to ensure effective removal of radioactive contaminants.

By implementing redundant safety systems, SMRs can achieve a high level of safety and reliability, minimizing the risk of accidents and protecting public health and the environment. The additional redundancies in SMRs are particularly important in urban environments where the consequences of a nuclear incident could be more severe due to the proximity of populated areas.

1. ***Conclusion:***

In conclusion, the transition from prescriptive to performance-based regulatory oversight marks a pivotal shift in addressing security challenges within Indian Small Modular Reactors (SMRs). This evolution underscores a proactive approach, emphasizing adaptability and efficiency in safeguarding nuclear facilities. By prioritizing performance metrics over rigid regulations, stakeholders can tailor security measures to suit the unique landscape of SMRs, thereby enhancing overall effectiveness while optimizing resource allocation. This strategic shift not only ensures compliance with evolving security standards but also fosters a culture of continuous improvement and resilience against emerging threats. As India embraces this progressive paradigm, it positions itself at the forefront of nuclear security innovation, paving the way for safe and sustainable nuclear energy development in the years to come.

***References:***

1. Atomic Energy Regulatory Board (India) Safety Code; Site Evaluation of Nuclear Facilities; [Code No. AERB/NF/SC/S (Rev.1)]
2. 61 FR 65157, Reactor Site Criteria Including Seismic and Earthquake Engineering Criteria for Nuclear Power Plants, December 11, 1996.
3. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5); IAEA Nuclear Security Series No. 13
4. Position Paper on “Physical Security for Small Modular Reactors” by National Energy Institute; July 31, 2021
5. Duguay, Raphael (2020) "Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats," International Journal of Nuclear Security: Vol. 7: No. 1, Article 2. <https://doi.org/10.7290/ijns070102>
6. Physical Protection Recommendations for Small Modular Reactor Facilities Alan Evans, Commie Byrum, Dennis Stanford, Emily Sandt, Tommy Goolsby; SANDIA REPORT: SAND2021-15712
7. Applicability of IAEA Safety Standards to Non-Water-Cooled Reactors and Small Modular Reactors; Safety Reports Series No. 123; International Atomic Energy Agency, Vienna, 2023
8. Nuclear Safeguards, Security, and Non-proliferation Achieving Security with Technology and Policy; 2nd Edition - February 15, 2019; Editor: James Doyle; Butterworth-Heinemann is an imprint of Elsevier, ISBN: 978-0-7506-8673-0
9. The Design and Evaluation of Physical Protection Systems; Second Edition; Mary Lynn Garcia, CPP; Sandia National Laboratories; Butterworth-Heinemann is an imprint of Elsevier; ISBN-13: 978-0-7506-8352-4