NUCLEAR ENERGY INSTITUTE

POSITION PAPER

# PHYSICAL SECURITY FOR SMALL MODULAR REACTORS

*July 31, 2012*

***ACKNOWLEDGMENT***
This NEI Position Paper was developed by the NEI
Small Modular Reactor Licensing Task Force.

POSITION PAPER

# PHYSICAL SECURITY FOR SMALL MODULAR REACTORS

## I. Introduction

This white paper addresses the security needs and requirements of near term Small Modular Reactors (SMRs).

This paper focuses primarily on integral pressurized water reactors (iPWRs), since the US Nuclear Regulatory Commission (NRC) expects to receive applications for licensing this type of SMR in the near future.

The goal is that the near term SMRs meet performance based outcomes consistent with current regulations.

Issues covered herein span the spectrum of safety/security integration into the design of SMRs, use of security performance standards for implementation, execution of a performance based licensing process, security staffing, cyber security and beyond design basis events (e.g., Aircraft Impact and Loss Of Large Areas[1]).

This paper provides a high level discussion of these issues which may later be applied to specific SMR designs. These issues, including protective strategies, will be addressed early, in technology specific pre-application meetings with the NRC, so that maximum efficiencies can be realized in the design, fabrication, installation and operation of SMRs, thus providing a "high-assurance" of safety.

A review of the current security regulations suggests that there is no need for rulemaking. However, on a technology-specific basis a reactor vendor may seek exemptions to certain regulations on a case-by-case basis focusing on performance based outcomes.

## II. Scope of Issues

SMRs designed to meet the needs for economical electric power, water desalination, hydrogen production, and process heat hold significant promise in meeting US energy needs. However, successful development and deployment of these new technologies requires commensurate and timely regulatory involvement.

The current NRC policy for SMR security and safeguards as stated in SECY-11-0184[2] indicates that for SMRs, it is expected that SMR vendors and licensees will achieve regulatory compliance

---

[1] Loss of Large Area will be the subject of a future NEI paper.
[2] SECY-11-0184 "Security Regulatory Framework for Certifying, Approving, and Licensing Small Modular Nuclear Reactors (M110329)", December 29, 2011 (see Summary).

within the existing regulatory framework through a thorough mutual understanding of requirements and compliance developed in Design Centered Working Group (DCWG) and pre-application meetings held with the NRC. This approach should optimize the use of industry and NRC resources.

## III. Description of Current Regulatory Framework

NRC regulations affecting physical security are primarily identified in 10 CFR Part 73 – Physical Protection of Plants and Materials. The applicable portions of 10 CFR Part 73 are defined in Appendix 1.

In addition, regulations addressing specific technical issues affecting security include portions of 10 CFR Part 50. The applicable portions of 10 CFR Part 50 are defined in Appendix 1.

These security and safeguards regulations were developed and evolved over several decades of experience with the large LWRs comprising the US fleet of power reactors.

## IV. Analysis of Regulatory Issues / Applicability to SMRs

### A. Technical Differences Enhancing SMR Physical Security

Some of the same features which are being included in the design of SMRs as safety/security improvements will also serve to reduce their vulnerability to physical threats. One feature common to many SMR designs is a compact reactor coolant boundary, contained mostly within the reactor pressure vessel (RPV). This feature enhances the safety of SMRs, in that Large Break Loss of Coolant Accidents (LOCAs) may not need to be postulated for these reactor types. This is different from the current fleet of power reactors and the current generation of new plants being installed.

Another feature common to many SMRs is an increased number of passive physical barriers and greater simplicity in systems required for safe shutdown. These vary between the designs, but include such features as RPVs and containment vessels located entirely underwater or below grade, the reactor building located partially or completely below grade, and fewer safe shutdown systems and components requiring physical protection. SMR designs incorporating security considerations beginning with the conceptual phase through design implementation provide features which deter and delay adversarial actions. The below grade installation of near term SMRs provide additional security benefits, such as minimizing aircraft impact, limiting access to vital areas and limiting the communication ability of adversaries. These same features may provide an excellent means of enhancing security system effectiveness against radiological sabotage. Application of the traditional multilayered defensive approach of deterrence, detection, assessment, delay, and interdiction can be used effectively for physical protection of SMRs. Deterrence, detection, and delay concepts are being addressed in the early design phase of a facility in order to provide sufficient response time for on-site security force response.

SMRs generally have lower power densities and larger heat sinks leading to a longer time period before design basis accidents result in exceeding fuel thermal limits. The combination of these lower thermal densities and the available passive heat removal paths reduces the need for operator actions during a postulated accident.

Safe shutdown of SMRs generally requires little immediate operator action (i.e. scram the reactor), after which natural circulation and heat transfer to a large pool of water will remove the decay heat and prevent fuel damage for the next several days with no operator action. This greatly reduces the likelihood of the control room being the target of an attack.

These features have been designed into many SMRs to increase safety and reduce the reliance on active components and they may also serve to reduce the number of target set elements needing incorporation into the site's physical protection program.

The ability to rely on a sufficient and effective onsite response to a security threat is a key factor that should be considered at the initial conceptual design phase to ensure sufficient intruder delays are included.

Some examples of methods for extending adversary delay times that can be incorporated into SMR designs include:

- Locate and configure vital components such that gaining access to these items is extremely difficult and time consuming for an intruder

- Locate and configure critical safety systems such that there is not a capability to destroy a target set from a single location

- Incorporate multiple layers of intruder delay barriers into the design and minimize the number of access points to areas containing vital assets

Upon examination of the various technologies utilized in the design of SMRs, it is evident that there is a substantial difference between these new designs and existing LWR technology sufficient to justify a "bottoms-up" assessment of physical protection and safety.

Not only is integration of security and safety in the early design phase of SMRs expected by the NRC[3], it is also more efficient and effective. Physical security system design considerations which minimize human involvement in security events (i.e., lower security risk profile), minimize impact of necessary future system modifications, and maximize adversary delay times should be addressed. Examples include:

- Designing the facility with limited (minimized) access points and multiple passive barriers based on a defense-in-depth approach to physical security

- Use of highly redundant detection, assessment and delay systems

---

[3] SECY-10-0034, "Potential Policy, Licensing, and Key Technical Issues for Small Modular Nuclear Reactor Designers", March 28, 2010.

- Use of enhanced weapons[4]

- Plan for use of modular capabilities in physical security systems to minimize impact on station security staffing for system maintenance as well as upgrades needed to address system technology obsolescence and potential future increased design basis threats

## B. Regulatory Issues Affecting SMR Physical Security

The regulatory issue of primary importance related to physical security of SMRs is security staffing. This issue has the potential to adversely affect the viability of SMR development in the U.S. Security staffing directly impacts annual operations and maintenance (O&M) costs and as such constitutes a significant financial burden over the life of the facility. Security staffing has become a major driver in operations and maintenance costs for operating plants. For this reason, evaluation of security staffing requirements for SMRs has become a key focal point.

SMRs have distinct advantages over current operating plants for improving security efficiency. SMRs are significantly smaller in size and system complexity which translates to smaller target sizes and smaller number of target set elements and target sets. These advantages may translate into a significant improvement of security staffing economics since the desired security and safety outcomes may be achieved with lower numbers of security staff.

Security staffing requirements are both stated and implied in the various physical security related CFR sections listed in Appendix 1 of this document. These requirements, many of which are based on years of operating experience with large LWR facilities, may not be appropriate or necessary for SMRs due to the simpler, safer and more automated design characteristics of SMRs. SMRs generally should have smaller owner controlled areas and vital areas, and a smaller number of target sets, as compared to conventional LWR facilities.

Key features of the physical protection programs that affect staffing expectations for nuclear facilities include:

- Defense in depth using graded physical protection areas: Owner Controlled Area, Protected Area, and Vital Area, with associated barriers and controls

- Access authorization programs

- Robustness of intrusion barriers

- Alarm assessment to distinguish between false or nuisance alarms and actual intrusions and to initiate response

- Likely response to intrusions

---

[4] *See* NRC Draft Reg. Guide DG-5020, "Applying for Enhanced Weapons Authority, Applying for Preemption Authority and Accomplishing Firearms Background Checks under 10 CFR Part 73"

- Planning for design basis threats that may evolve over the facility lifetime
- Integrated Response Planning (IRP) with Federal, state, and local responders.

The integration of security into the design at an early stage coupled with a performance based approach and optimized use of automation in security systems with adequate backup contingencies designed to minimize human interaction in security events should be considered when assessing security staffing requirements for SMRs. A reduction in the security staffing requirements may be appropriate if such an approach is taken.

Another physical security related regulatory issue of significance to SMRs is Aircraft Impact Assessment (AIA). SMRs will utilize existing industry guidance, including US NRC Reg. Guide 1.217[5] endorsing NEI 07-013, "Aircraft Impact Assessments" and NRC Inspection Procedure Number 37804 "Aircraft Impact Assessment."

Because of the small size of SMRs, assessment of Loss of Large Areas (LOLA) may require special attention. Current guidance is provided in NEI 06-12, as supplemented by Interim Staff Guidance DC/COL-ISG-016 "Compliance with 10 CFR 50.54(hh)(2) and 10 CFR 52.80(d)." This aspect of SMR licensing is both standard design and site- specific and therefore should be addressed in pre-application meetings. LOLA will be the subject of a future NEI paper.

The cyber security requirements of 10 CFR 73.54(a)(2) require licensees to protect such systems and networks from cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems, or data; and impact the operation of systems, networks, and equipment. Regulatory Guide 5.71 "Cyber Security Programs for Nuclear Facilities" provides guidance for complying with 10 CFR 73.54(a)(2), which can be utilized in pre-application meetings to reach agreement on the design of systems and networks for SMRs. Additional guidance is provided in NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors."

### C. The Use of PRA to Inform SMR Physical Security

The significant differences in safety and security design features between SMRs and large LWRs support innovative approaches to establishing SMR physical security planning.

In the discussion on *Security and Safeguards Requirements for SMRs* of SECY-10-0034, the NRC states that SMR designers are expected to integrate security into the design.

The current Aircraft Impact Rule (74 FR 28112) requires new nuclear power reactors to perform rigorous assessments to identify and incorporate those design features and functional capabilities that could provide additional inherent protection to avoid or mitigate effects of an aircraft impact. Applicants are required to demonstrate that with reduced operator actions:

[5] US NRC, Regulatory Guide 1.217, "Guidance for the Assessment of Beyond-Design-Basis Aircraft Impacts", Nuclear Regulatory Commission, Washington, D. C., August 2011.

1) the reactor core remains cooled or the containment remains intact

2) spent fuel pool cooling or spent fuel pool integrity is maintained

The methods employed in measuring and documenting compliance with regulatory requirements will need to account for the overall integrated security plan that addresses many aspects of SMR safety / security. It must fully address plant inherent safety design features, site arrangement, and more focused staffing plans.

The SMR nuclear security challenge is fundamentally one of risk management and it is necessary to make risk informed decisions from the inception of the individual plant design and licensing process. Tools, such as Probabilistic Risk Assessment (PRA), are being used to inform SMR security design. Groundwork for incorporation of such an approach for Nuclear Power Plant (NPP) security has been done by Sandia National Laboratories in SAND2007-5591[6].

It has been NRC's policy since 1995 that use of PRA should result in a regulatory approach that integrates and optimizes reactor safety, security, and preparedness through risk management (NRC News S-05-012) [7]. The use of risk analysis and risk insights is essential to achieve success in both plant design and regulatory arenas. Security concerns, including terrorist threats, raise many of the same issues involved in avoiding and mitigating reactor accidents, and will play an important role in bringing design-related security issues to the forefront of the design phase.

PRA is the most systematic, comprehensive and tested approach to address these complex, interrelated issues. By using PRA insights in conjunction with a defense-in-depth deterministic approach, enhanced security may be able to be introduced as a fundamental design criterion in preserving safety margins. Accommodating these methodologies at the conceptual design phase may be the most efficient way to assure they are an integral part of the final design and far more economical than integrating an evolving requirement later.

Sandia National Laboratories has authored numerous guidance documents and technical manuals that provide information necessary to analyze and optimize physical protection in the design of DC/COL power plants. The SMR plant security assessments should be conducted by reliance on the SMR technology-specific design features as informed by the plant-specific PRA and plant security plans should be developed by applying the performance based security licensing bases. The above described process of risk-informed performance based security assessments could be conducted during the entire design and licensing process of SMRs.

### D. Financial Issues Affecting SMR Physical Security

A primary financial issue relating to physical security for SMRs is security staffing. As discussed in Section 4b, security staffing has the potential to be a significant O&M cost. A

[6] D. W. Whitehead, C. S. Potter and S. L. O'Connor, Nuclear Power Plant Security Assessment Technical Manual, SAND2007-5591, Sandia National Laboratories, Albuquerque, NM, September 2007.

[7] Nils J. Diaz (Chairman, US NRC), "The Role of Risk Management in Regulation (Where we are and where we should be going)", NRC News No. S-05-012, *International Topical Meeting on Probabilistic Safety Analysis (PSA '05)*, US Nuclear Regulatory Commission, September 12, 2005.

robust development and deployment of SMRs in the US hinges on cost and risk certainty. Establishing the appropriate security staffing, without compromising nuclear safety and security, is a necessary component in demonstrating the economic viability for SMRs. Fundamentally, plant staffing including security staffing should be based on what is needed to ensure operational security and safety. The combination of smaller footprint, robust barriers, engineered delay, detection, and assessment features, inherent safety features, and the potential of both fewer target sets and target set elements may support reduced security staffing levels for SMRs.

Development of realistic, performance-based security planning appears to be the path offering the most potential in terms of security staff reductions for SMRs. Such planning should recognize and support the use of plant security design features and concepts which lessen dependence on security staff interdiction. Successful outcomes of such design features may require development and use of alternative performance assessment techniques. Although there may be additional initial costs for development of such systems, these costs are expected to be offset by minimizing security related O&M costs through reduced on site security staffing.

## V. Suggested Regulatory Issues Framework for SMRs

It is conceivable that application of current regulatory guidance for some SMRs will require additional performance based justifications to conform but will not require deviation from the fundamental acceptance criteria or performance based outcomes. In some cases, alternative measures or exceptions to current applicable regulations may be required. Exceptions from current regulatory requirements in such cases may be justified by sound technical argument. The conformance to current regulatory guidance and/or exceptions to regulations will be addressed in technology-specific pre-application meetings. A thorough review of regulations and regulatory guidance for SMRs (with possible revisions to some guidance documents) will assure performance outcomes are met consistent with regulations.

In the context of security regulatory issues for SMRs, it is believed that the current licensing framework can be utilized with appropriate technical justification for exceptions as needed. SMR applicants will take advantage of the inherent safety and security features to demonstrate that the level of protection offered equals or exceeds current regulatory requirements. The nuclear industry will continue to work with the NRC in a transparent process that allows for addressing the various technical needs in the security area. One approach that has been proven beneficial is the development of topical reports that address specific aspects of security related design and operations.

## VI. Conclusions and Recommendations

In conclusion, both realistic and reasonable security planning requirements for SMR designs can be based on current regulatory requirements with exceptions or alternative measures as needed. Development of realistic technology-specific based acceptance criteria and outcomes for security regulations is recommended as the path offering the most potential in terms of increased safety margins, enhanced security and improved efficiencies for SMRs.

Performance based security assessments may be developed using risk-informed plant design features which will demonstrate that physical, staffing, and technological design requirements are fully integrated throughout the entire design and licensing process.

Regulators and the nuclear industry should adopt a performance outcomes-based approach for all SMRs within the existing regulatory framework that recognizes and incentivizes the reduced security risk exposure expected due to the SMR integrated safety and security features.

Regulators and the nuclear industry should continue dialog on enhancing the security posture for SMRs through the use of DCWGs comprised of industry and regulator representatives. This recommended approach would provide a transparent process for addressing the various technical aspects specific to SMRs and allow for the preparation of application-specific assessments and topical reports, as needed.

## VII. Appendices

### Appendix 1 – Defining of applicable existing regulatory requirements

**General Provisions**

- 73.20 General performance objective and requirements.

**Physical Protection Requirements at Fixed Sites**

- 73.40 Physical protection: General requirements at fixed sites.
- 73.45 Performance capabilities for fixed site physical protection systems.
- 73.46 Fixed site physical protection systems, subsystems, components, and procedures.
- 73.50 Requirements for physical protection of licensed activities.
- 73.51 Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste.
- 73.54 Protection of digital computer and communication systems and networks.
- 73.55 Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.
- 73.56 Personnel access authorization requirements for nuclear power plants.
- 73.57 Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information.
- 73.58 Safety/security interface requirements for nuclear power reactors.
- 73.59 Relief from fingerprinting, identification and criminal history records checks and other elements of background checks for designated categories of individuals.
- 73.60 Additional requirements for physical protection at nonpower reactors.
- 73.61 Relief from fingerprinting and criminal history records check for designated categories of individuals permitted unescorted access to certain radioactive materials or other property.

**Appendices to 10 CFR Part 73**

- Appendix B – General Criteria for Security Personnel

- Appendix C – Nuclear Power Plant Safeguards Contingency Plans
- Appendix G – Reportable Safeguards Events
- Appendix H – Weapons Qualification Criteria
- Appendix I – Category 1 and 2 Radioactive Materials

In addition, regulations addressing technical issues affecting security include the following.

- Part 50.150 - Aircraft Impact Assessment
- Part 50.54(hh)(2) - Conditions of Licenses (Loss of Large Areas)

■