Methodological Approach and Considerations for a Security Assessment to Demonstrate Compliance with the Performance Criteria of 10 CFR 73.55(TBD)

Prepared by the Nuclear Energy Institute
[Month] 2020

Acknowledgements

This technical report was prepared by the Nuclear Energy Institute (NEI). We greatly appreciate the efforts by our members and other organizations that contributed to the preparation and review this document.

NEI Project Lead: David Young

Table of Contents

1 PURPOSE

This technical report provides guidance for performing a security assessment to demonstrate that a nuclear power reactor applicant qualifies for the voluntary, performance-based alternatives to certain physical security requirements contained in Title 10 of the Code of Federal Regulations (10 CFR) 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." To qualify for the alternative requirements, an applicant must demonstrate that the nuclear power reactor facility meets one of the performance criteria specified in 10 CFR 73.55(TBD). The guidance in this report addresses security assessments targeted at any of the three performance criteria listed in 10 CFR 73.55(TBD).

2 SECURITY ASSESSMENT GUIDELINES

2.1 Threat Characteristics

The threat to be considered in a security assessment is the design basis threat of radiological sabotage as stated in 10 CFR 73.1, "Purpose and scope," and referred to as the DBT.[1] Assessment elements involving consideration of specific DBT capabilities and tactics should be informed by the guidance in Regulatory Guide (RG) 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements."[2] An applicant may use an alternative approach to a given capability or tactic in their assessment; however, the alternative approach should be clearly identified and supported with a technical basis.

2.2 Probabilistic Risk Assessment Information

A security assessment may consider information available from a probabilistic risk assessment (PRA) developed to meet facility licensing requirements (e.g., evaluation of severe accidents) established by the U.S. Nuclear Regulatory Commission (NRC). Prior to beginning the assessment, an applicant is encouraged to become familiar with the guidance in RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors." RG 5.81 includes a discussion on the use of PRA information and insights to assist with the identification of target sets. This material can help inform the content of a security assessment performed to demonstrate compliance with 10 CFR 73.55(TBD).

RG 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," provides an approach that the NRC has found acceptable for developing a probabilistic risk assessment (PRA) suitable for risk-informed regulatory decisions. The guidance in RG 1.200 should be followed to the extent practical and applicable when assessing the acceptability of probabilistic risk information used in a security

[1] An applicant planning to assess a threat with characteristics different than the DBT (e.g., one with less capabilities) should also seek an exemption from this requirement as part of the facility's licensing process.
[2] RG 5.69 contains Safeguards Information (SGI) and is therefore not publicly available.

assessment.

2.3 Plant Configuration/Mode Changes

As applicable to the facility design and features, a security assessment should consider the effects from planned (routine) changes to the plant configuration, or mode of operation, on the ability to continuously meet a targeted performance criterion. If needed, the assessment should describe the controls that will be implemented to ensure that the performance criterion will always be met. Alternatively, a security assessment could be directed at two (or all three) performance criteria whereby one performance criterion is met in one plant configuration or mode, and another criterion is met in a different configuration or mode.

2.4 Definition of Target Set and Relationship to Performance Criteria

As used in this document:

- A "target set" is the minimum combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in offsite doses greater than the reference values in 10 CFR 50.34 and 52.79.

- An "achievable target set" means a target set that is within the ability of the DBT to compromise, destroy, or render nonfunctional, absent actions by an onsite armed response force.

The relationship of a target set to the three performance criteria presented in 10 CFR 73.55(TBD) is shown below.

Performance Criterion	Facility Target Set?	Achievable Target Set?	Mitigation Measures for Loss of Target Set?
[#1]	No	N/A	N/A
[#2]	Yes	No	N/A
[#3]	Yes	Yes	Yes

The material in RG 5.81 can help inform the identification and development of target sets.

2.5 Credit for Manual Actions

A manual action performed by the facility staff may be credited[3] in a security assessment intended meet Performance Criterion [#2] or Performance Criterion [#3], including actions to prevent or mitigate offsite radiological consequences. The basis for assuming action performance should provide reasonable assurance that the action could be completed under the postulated attack conditions and be documented in the assessment. For example, an action to enable a physical protection element, such as changing the position of a barrier or arming a delay feature, could be credited provided the facility's layout, staffing and physical security features give reasonable assurance of its completion during an attack. Guidance for assessing the credibility (and thus acceptability) of a proposed manual action can be found in RG 5.81.[4]

Manual actions initiated from a remote location may also be credited. In these cases, the basis should also address potential challenges to timely performance of the action and mitigative measures. Topics to consider include cyber attacks, reliability and redundancy of communications systems, and potential collateral duties of personnel at the remote location.

2.6 Credit for Law Enforcement Support

A security assessment may credit an onsite response from a law enforcement agency to neutralize the threat; this credit may be applied in an assessment targeted at any of the three performance criteria. The scope and timing of the law enforcement response should be consistent with the Reasonable Assurance of Protection Time (RAPT) described in RG 5.76, "Physical Protection Programs at Nuclear Power Reactors." It is possible that a response time shorter than the RAPT could be used; however, the security assessment would need to include a site-specific basis for the shorter time. [*Augment this information with discussion in pending SECY on RAPT/SBT.*]

2.7 Safety/Security Interface

The performance of physical protection elements described in a security assessment must be consistent with the requirements in 10 CFR 73.58, "Safety/security interface requirements for nuclear power reactors." More specifically, the design and performance of these elements cannot adversely affect reactor safety and, conversely, plant and operator responses to the event (e.g., changes in equipment configuration) cannot adversely affect physical protection elements. Further guidance on this topic can be found in RG 5.74, "Managing the Safety/Security Interface."

[3] For the purpose of this document, "credit" means a determination that a proposed action or activity can be performed during an attack, thereby permitting the action or activity to be relied upon to support conclusions in the assessment. The determination should meet a "reasonable assurance" standard.
[4] RG 5.81 uses the term "operator action."

2.8 Hazards from Adjacent Facilities and Transportation Routes

When applicable, the security assessment should identify and evaluate hazards from an adjacent non-nuclear facility that could potentially affect the safety or security features relied upon to meet a performance criterion. The assessment should also examine similar hazards emanating from an onsite or nearby transportation route (e.g., a roadway or rail line). Consideration should be given to hazardous conditions created by the DBT as well as those arising from other causes. Potential hazards to consider include:

- Steam releases
- Chemical explosions, releases or spills
- Fires
- Misuse of industrial radiation sources

The characteristics of each hazard, such as timing, severity, and persistence, should be determined. The assessment should then describe the design provisions and/or response actions that will mitigate the impacts of each hazard and ensure that the capability to meet the performance criterion is maintained. Hazard analyses performed to meet other NRC licensing requirements (e.g., reactor siting criteria) may be referenced as applicable; there is no need to perform duplicative analyses.

2.9 NUREG/CR-7145

Prior to beginning a security assessment, an applicant is encouraged to become familiar with the guidance in NUREG/CR-7145, "Nuclear Power Plant Security Assessment Guide." NUREG/CR-7145 provides guidance to design certification and combined license applicants for optimizing physical security during the design phase and minimizing reliance on operational programs (human actions). The material in NUREG/CR-7145 can help inform the content of a security assessment performed to demonstrate compliance with 10 CFR 73.55(TBD).

2.10 Use of Security Modelling Tools

An applicant may employ a computer application in a security assessment to model the security-related aspects of an attack on the facility. For example, an application could be used to evaluate the detection and delay capabilities described in the assessment. For additional information on security assessment modeling tools, see Sandia National Laboratories Report SAND2007-5591, "Nuclear Power Plant Security Assessment Technical Manual."

3 PERFORMANCE CRITERIA

3.1 Performance Criterion [#1] (*regulatory reference later*)

Performance criterion [#1] states:

> The radiological consequences from a hypothetical, unmitigated event involving the loss of engineered systems for decay heat removal and possible breaches in physical structures surrounding the reactor, spent fuel, and other inventories of radioactive materials result in offsite doses below the reference values defined in 10 CFR 50.34 and 52.79.

To meet this performance criterion, a facility must have no combination of equipment or operator actions that, if prevented from performing their intended safety function or prevented from being accomplished, would likely result in offsite doses exceeding the cited reference values (i.e., the facility does not have a target set). An applicant can demonstrate compliance with this criterion through a security assessment based on a consequence analysis that determines offsite doses for the postulated security event. The assessment may consider all engineered safety and security features in place at the beginning of the event; manual actions to operate these features after the attack has begun should not be considered.

Guidelines for performing a consequence analysis are presented in section 4 of this document.

3.2 Performance Criterion [#2] (*regulatory reference later*)

Performance criterion [#2] states:

> The plant features necessary to mitigate an event and maintain offsite doses below the reference values in 10 CFR 50.34 and 52.79 cannot reasonably be compromised by the design basis threat of radiological sabotage.

To meet this performance criterion, a facility must have no achievable target set that would likely result in offsite doses exceeding the cited reference values; in other words, the facility does not have a target set that can be compromised by the DBT (given their capabilities) to an extent necessary to result in offsite doses exceeding the cited reference values. An applicant can demonstrate compliance with this criterion through a security assessment that identifies plant target sets and demonstrates the capability of safety and security features to prevent the DBT from compromising any target set. To meet this criterion, the assessment results cannot rely upon actions by an onsite armed response force.

Security features that may be considered in the assessment include:

- Access control measures
- Detection and assessment capabilities

- Delay and barrier features
- Actions by the facility staff or performed remotely
- Insider threat mitigation

3.3 Performance Criterion [#3] (*regulatory reference later*)

Performance criterion [#3] states:

> Plant features include inherent reactor characteristics combined with engineered safety and security features that allow for implementation of a mitigation strategy if a target set is compromised, destroyed, or rendered nonfunctional, such that offsite radiological consequences are maintained below the reference values defined in 10 CFR 50.34 and 52.79.

To meet this performance criterion, a facility should have a reactor design with a large heat capacity and slow progression from loss of safety equipment to degradation of fission product barriers and release of radionuclides from the facility. An applicant can demonstrate compliance with this criterion through a security assessment based on a consequence analysis that determines the shortest elapsed time from event initiation to the onset of conditions that would produce a release with radiological consequences exceeding the cited reference values. The assessment will also need to describe the planned mitigation strategies that would be implemented, within the time available, to prevent the conditions leading to the radiological release.

Guidelines for performing a consequence analysis are presented in section 4 of this document.

A “strategy” should be understood as a plan of action for maintaining or restoring a safety function that is challenged due to the loss of a target element or target set. A strategy can be implemented by one or more methods. A “method” is a series of actions designed to implement a specific strategy. As an illustrative example of these terms, consider that placing a portable pump in service (a method) to inject water into a reactor vessel (a strategy) would maintain or restore the core cooling safety function.

The description of a mitigation strategy should identify the safety function performed, the events that would prompt implementation, the anticipated time for performance (with consideration of reasonably expected conditions prevailing during an attack), and the following elements needed for execution, as applicable.

- Equipment (e.g., portable pumps, generators, hoses, cables, etc.)
- Storage locations (onsite and/or offsite)
- Transport and deployment arrangements (i.e., provisions for moving the equipment from a storage location to the location where it will be placed into service)

- Key actions to place equipment in service
- Staffing
- Communications

A facility meeting performance criterion [#3] will need to perform periodic administrative and maintenance activities that support the ongoing capability to implement mitigation strategies. To this end, the security assessment should discuss the following items.

- Anticipated or actual documentation of support from offsite resource providers (e.g., letter of agreement, memorandum of understanding, contract, etc.) and how this documentation will be periodically verified and updated.
- Plant design change and configuration control measures to ensure that credited strategies can be readily implemented or modified as needed.
- Maintenance and testing of equipment.
- Training and drills to validate strategies and maintain proficiency of personnel.

An applicant complying with the requirements of 10 CFR 50.155, "Mitigation of beyond-design-basis events," is encouraged to become familiar with the guidance in RG 1.226, "Flexible Mitigation Strategies for Beyond-Design-Basis Events." RG 1.226 identifies methods and procedures the NRC staff considers acceptable for nuclear power reactor applicants and licensees to demonstrate compliance with NRC regulations covering planning and preparedness for beyond-design-basis events. The material in RG 1.226 can help inform the content of a security assessment performed to demonstrate compliance with performance criterion [#3].

4 CONSEQUENCE ANALYSIS GUIDELINES

4.1 General Instructions and Assumptions

For the purpose of this document, a consequence analysis is an activity performed by the applicant to determine radiation doses at the boundary of the exclusion area and the boundary of the low population zone. As noted above, a consequence analysis will be needed to support demonstration of compliance with Performance Criteria [#1 and #3]. The analysis should describe the initiating event (i.e., the actions taken by the DBT), the compromised target set (for assessments directed at Performance Criterion [#3]), and the subsequent responses by the plant, facility staff and supporting organizations and agencies, including law enforcement. With this information, the analysis should then determine the type and amount of radioactivity released to the environment.

The following assumptions should be employed in a consequence analysis.

a. Both active and passive safety features may be considered in the analysis.

b. The atmospheric release pathway is the risk-dominant contributor to offsite doses (i.e., no consideration of direct exposures from the facility or releases to liquid pathways is necessary).

c. The atmospheric release consists of aerosols or gasses (with radioactive decay and in-growth corrections as appropriate). If a release pathway requires more complex atmospheric transport modeling, additional analyses may be needed.

d. A straight-line Gaussian plume segment-type atmospheric dispersion model, with modifications as needed to account for near-field dispersion phenomena, is used to estimate atmospheric concentrations. Such models are generally most suitable for relatively simple transport situations, such as open and level terrain, relatively steady meteorology, and relatively close distances (<10 km). Use of a more advanced dispersion model may require a different set of assumptions or methodological steps than those described in this document.

   For facilities with relatively small exclusion areas, a straight-line Gaussian plume model may overestimate near-field radiological consequences. In these cases, other consequence analysis models may be used.

e. There is no credit for pre-planned offsite protective actions such as evacuation or sheltering.

f. The exposure durations should be consistent the durations specified in 10 CFR 50.34(a)(1)(ii)(D)(1) and (2), or 10 CFR 52.79(a)(1)(vi)(A) and (B).

g. The analysis need not postulate coincident events (e.g., a seismic or flooding event), or failures of structures, systems or components unrelated to the event.

For the release scenario and dose projections, a quantitative radiological source term should be developed by specifying atmospheric release characteristics such as the time dependent isotopic release rates to the atmosphere, release durations, release locations, physical/chemical form, plume buoyancy, etc. The radiological source term should be estimated using analysis methods and codes evaluated by an NRC-accepted process. In cases where more than one release scenario is identified, the consequence analysis should use the scenario (i.e., the event sequence) that produces the greatest offsite dose at the boundaries of the exclusion area and low population zones.

4.2 Meteorological Parameters

An analysis to develop meteorological data may be needed to evaluate a range of meteorological conditions in a probabilistic fashion. Alternately, conservative transport and dispersion conditions may be assumed, although the conservatism of the selected conditions should be evaluated to ensure that the combination of parameters selected for transport and dispersion modeling was in fact conservative. For example, with appropriate justification, site-

specific meteorological information could be used to develop average expected atmospheric dispersion characteristics (i.e., 50th percentile meteorology for the site), which would then be employed in the analysis.

Selection of a source of meteorological data would include an evaluation of data needs such as wind speeds, atmospheric stability, precipitation, mixing height, etc., for temporal and geographical representativeness. The quality and completeness of the meteorological data should be assessed, and significant uncertainties identified and characterized. It is expected that site-specific meteorological data will be used; however, there may be instances where site-specific data is not available or of sufficient quality and completeness. In these cases, there should be an explanation of the appropriateness of the meteorological data used for the analysis.

4.3 Atmospheric Transport Modeling

An atmospheric transport model appropriate for the range of distances under consideration should be identified. For Gaussian-type models, dispersion parameters appropriate to the characteristics of the area and distance ranges under consideration should be identified, and conceptual approaches for the treatment of near-field effects such as elevated releases, building wake effects, plume meander, plume rise, etc. should also be identified. The selection of an atmospheric transport model should also involve selection of a conceptual approach for treatment of wet and dry deposition. Any assumptions made in the atmospheric transport model should be identified.

4.4 Exposure Parameters

The relevant exposure pathways should be identified; for example, exposure to both airborne and deposited radioactivity from atmospheric releases would involve both external (groundshine and cloudshine) and internal (inhalation of airborne material during cloud passage or as a result of resuspension) exposure. In order to assess the dose, the exposure parameters (e.g., shielding factors, breathing rates, exposure durations, etc.) would need to be characterized. Dose estimations should be carried out by combining the results of the release, transport, and exposure assessment with a recognized source of dose conversion factors (such as Federal Guidance Reports issued by the U.S. Environmental Protection Agency) to estimate the doses at the boundaries of the exclusion area and low population zone.

5 UPDATES

As needed, a security assessment should be updated to reflect changes to facility features or offsite support resources described in the assessment. The NRC should be notified of a change that affects compliance with an applicable performance criterion (e.g., an anticipated change will result in the performance criterion no longer being met).

Documentation of support from offsite resource providers should be verified on an annual basis.