ADVANCED REACTOR SAFEGUARDS & SECURITY

Topical Report for DMA

FY26 ARSS Spring Program Review

PRESENTED BY

Steven Horowitz

April 28-30, 2026

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2026-19489PE

Deliberate Motion Analytics (DMA)

- An algorithm that uses the deliberate motion of targets within a sensor's field of view to differentiate alarms caused by an intruder from those caused by other natural sources
- Fuses multiple complementary sensors, such as radar, passive radio frequency, lidar, sonar, and video, to provide reliable detection
- Sandia has conducted numerous iterations of testing the technology to demonstrate its ability to reduce nuisance alarm rates, detect intrusions "beyond-the-fence," and detect intrusions in water environments

Regulatory Paradigm

Regulatory Paradigm

- Physical protection requirements for commercial nuclear power plants (NPPs) in the US are included within Title 10 of the Code of Federal Regulations (CFR) Part 73
  - Parts 50 or 52 licensing pathways → 10 CFR 73.55 for protection against radiological sabotage (all existing commercial large LWRs use this)
  - Part 53 → 10 CFR 73.100 “Technology-inclusive requirements for physical protection of licensed activities at commercial nuclear plants against radiological sabotage”

Current Regulatory Guidance – RG 5.44

- Rev. 3 recommends the perimeter intrusion detection system to detect an individual with a minimum weight of 35 kg (77 pounds) walking, crawling, running, jumping, or rolling through the protected area perimeter
  - 90% probability of detection with an associated confidence level of 95%
  - Reduce false and nuisance alarms to one each per zone per day
  - False alarms are alarms for which a cause cannot be identified and may indicate a problem in the segment
  - Nuisance alarms are alarms that are expected to occur due to the proper functioning of the detection system to an initiating event not caused by a malicious event. In a nuisance alarm, the cause is known (e.g., animals, bugs, people, etc.).
- Rev. 4 (Forthcoming) – Info on novel systems
- RG 5.97 for Part 53 – Cites RG 5.44

Current Regulatory Guidance (Cont.)

- NUREG-1959, Revision 1 provides information on the design, installation, testing, maintenance and monitoring of intrusion detection systems, subsystems, and assessment systems
- This document does not provide information on novel detection or assessment systems, but
  - Provides methods for acceptance, performance, and operability testing of detection and assessment systems that are applied in the TR for DMA

Topical Report

- Analyzes regulatory paradigm for DMA
  - Part 50 and 52 (10 CFR 73.55)
  - Part 53 (10 CFR 73.100)
  - Discusses demonstration of DMA with respect to applicable regulatory guidance (RG 5.44 Rev. 3, RG 5.97 Rev. 0, and NUREG-1959, Rev. 1
- Summarizes existing test data

Topical Report (Continued)

- Topical report lists the potential need for exemptions and/or alternatives by the licensee for:

1. DMA to fulfill detection and assessment
2. Physical barrier requirements in the case of elimination of isolation zone and double fence line

- The analysis assumes baseline configuration and doesn't (yet) account for more advanced deployment considerations such as water intakes

Need for Exemptions/Alternatives

Need for exemptions and/or alternatives under the 10 CFR 73.55 licensing framework if DMA is used by a commercial NPP applicant to fulfill the detection and assessment functions

Regulation(s)	Exemption/ Alternative/Both	Comments
10 CFR 73.55(e)(7)(i) requires an isolation zone of sufficient size to permit observation and assessment on either side, and detect attempted and actual penetration of the protected area perimeter barrier before completed penetration	Exemption	Elimination of isolation zone will trigger a need for an exemption from this requirement.
Protected area perimeter must limit access into the protected area (10 CFR 73.55(e)(8)(i)(A)) and channel persons, vehicles, and materials to access control portals (10 CFR 73.55(e)(8)(i)(B))	Dependent on engineering design choices	Elimination of the traditional isolation zone and protected area boundary will trigger the need discussions of how this impacts access control requirements under the current NRC licensing framework. A single protected area fence line or barrier would allow for channeling of persons, vehicles, and materials.
10 CFR 73.55(e)(10)(i)(A) requires a vehicle barrier system and periodic surveillance and 10 CFR 73.55(e)(10)(i)(C) includes requirements for periodic surveillance of these barriers.	Dependent on engineering design choices	Typically, the vehicle barrier system is located within the protected area boundary. The licensee is still required to have a vehicle barrier system, and also demonstrate how it will detect tampering.
10 CFR 73.55(g)(1)(i)(A through C) requires licensees to locate access control portals outside or concurrent with the physical barrier system through which it controls access	Dependent on engineering design choices	The licensee will need an exemption and an alternative if both fences are eliminated. In the case of a single fence delineating the protected area, the licensee would meet these requirements by locating the access control function to the protected area outside or concurrent with it.
10 CFR 73.55(g)(1)(i)(E)) Individual responsible for last access control function	Dependent on engineering design choices	The applicant must describe how the last access control function into the protected area will be fulfilled, including the requirement to isolate that individual within a bullet-resisting structure. A single barrier along with DMA would allow for this without an exemption or alternative.
10 CFR 73.55(g)(2) and (3) granting access to authorized persons and vehicles into protected area. Conduct searches of individuals, vehicles, and materials in accordance with 73.55(h)	Dependent on engineering design choices	The licensee will need a sufficient technical basis demonstrating how it will control and facilitate access of approved individuals and vehicles into the protected area, and detect attempted unauthorized access in these portals.
10 CFR 73.55(g)(7 through 8) requirements for visitors and escorts	Alternative	The licensee must demonstrate its technical licensing basis for requirements for escorting individuals into the protected area and requirements for escorts.

Conclusion

- The use of DMA to perform the detection and assessment requirements in 10 CFR 73 for commercial NPPs is possible with a number of alternatives and/or exemptions, along with performance testing
- An applicant would be required to demonstrate adequate installation, maintenance, and system integration as well as limited-scope and system-level performance testing to achieve the performance requirements
- Cases where DMA replace a traditional perimeter intrusion detection system with an isolation zone and protected area perimeter will trigger the need for several exemptions to existing requirements in these areas

Backup Slides

NRC vs DOE Terminology

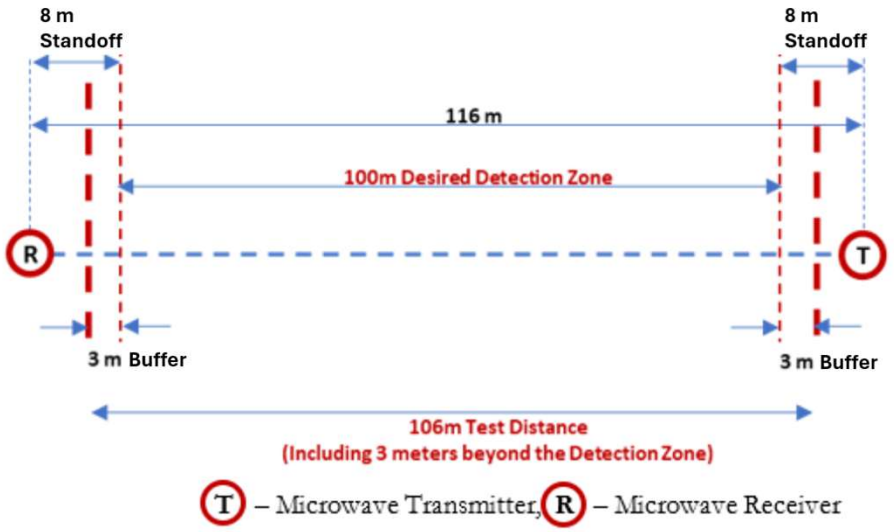
- “Detection” for the U.S. Nuclear Regulatory Commission’s terminology is commensurate with the Department of Energy’s (DOE’s) “sensing.” Where DOE refers to the combination of sensing with subsequent assessment as detection, NRC refers to detection separately from assessment.
- This paper uses NRC’s terminology throughout as the relevant regulatory authority.

Pertinent Regulatory Guidance

- Existing regulatory guidance for Perimeter Intrusion Alarm Systems exists within Regulatory Guide (RG) 5.44 Revision 3
- Proposed Rev. 4 discusses how licensees can demonstrate compliance with other technologies to fulfill the detection and assessment systems requirements in 73.55(i). Page 34 of Draft Guide (DG)-5065 states:
  - *2.9 Other Intrusion Detection Systems*
  - *2.9.1 Some systems currently under development may be acceptable, when fully developed, for use at NRC-licensed facilities.*
  - *2.9.2 Other systems that currently do not have an acceptable detection performance capability may at some future time be refined and be found suitable.*
  - *2.9.3 In either case, these systems would have to be performance tested by the licensee and a qualified independent agent (such as a national laboratory) before consideration by the NRC*

Performance Testing Prior to Deployment

- Begin with single zone
- Discretize intervals of detection
- Establish traversal method, speed, pathways
- Document alarms, including nuisance and false
- Note and consider varying times of day/weather (sunlight, humidity, temperature)



Performance Testing after Implementation (RG 5.44)

- Single performance test per week in place of a weekly operational test
- Eliminates the need for semi-annual performance testing
- Most vulnerable area of each segment is identified along with vulnerable associated weather conditions
- Each segment is tested over time using a combination of the vulnerable approaches
- At the end of the annual period, data is accumulated
- If a sensor has successful detections 50 times out of the 52-week period, additional performance testing is not needed. If not, the system must be assessed for issues and performance testing restarted
- In this option, traditional performance testing is still needed after detection system repairs or outages

Alternative Testing Program (RG 5.44)

- Each detection zone segment for a sensor system should be operationally tested once per week and performance tests conducted semi-annually
- The operational test should be conducted in a specific zone of detection selected at random
  - All zones should be operationally tested at least once within the seven-day period
- Performance tests should select the most vulnerable area of each segment as well as the associated method of adversary approach
- Associated weather conditions should be considered for consideration of which type of weather results in enhanced system defeat vulnerability
- A total of at least 30 tests should be conducted, with all 30 resulting in successful detections (results in satisfying the desired probability of detection of 90% with the associated 95% confidence interval)
  - If the minimum number of 30 successful detections is not achieved within 30 tests, the system should be evaluated for malfunctions

Assessment

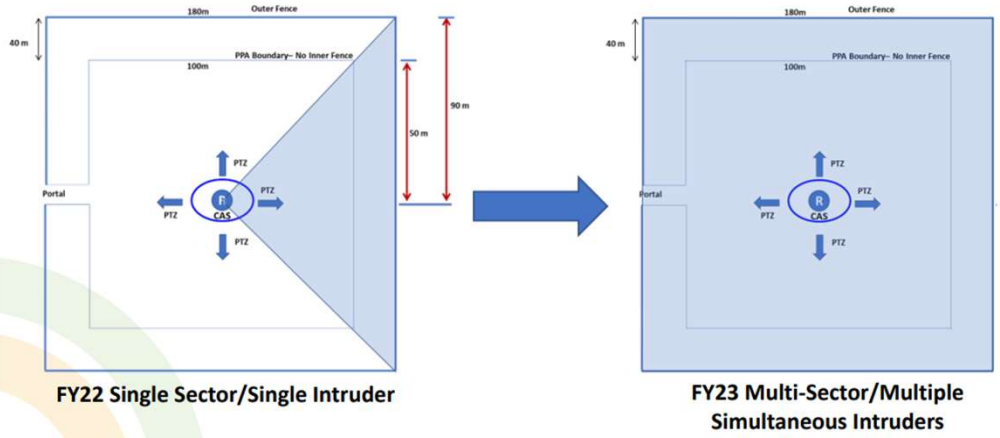
- RG 5.44 Rev. 3 describes two acceptable methods of assessment for licensees of commercial NPPs:

1. The first method includes fixed CCTV systems perpendicular to the intruder's anticipated path
   - These systems should transmit and display to the alarm stations recording of the initiating detection event as well as a period immediately prior to the detection
2. The second acceptable method is assessment via fixed guard posts, with each guard observing at most one direction of assessment zone and communicating immediately to both alarm stations

Engineering Considerations

Detection Zones

- Rev. 3 of RG 5.44 recommends the perimeter be segmented into lengths of 100 m zones
- DMA has historically been developed and proposed to function in a 360-degree detection envelope



- John "JR" Russell, "Security Systems of the Future for SMRs and Microreactors – FY23 Activities Update," October 31, 2023, SAND2023-11888PE.

Elimination of Segments

- RG 5.44 Rev. 3 mentions the licensee's use of detection zones divided into independently alarmed and uniquely monitored segments of no more than 100 m to facilitate assessment. While not a regulatory requirement, it is highly likely that this will impact the NRC's acceptance of DMA
- RG 5.44 mentions that a segment should also be limited by the ability of a single individual to observe the entire segment from one end
- The protected area boundary of a real-world facility is likely to have variances in topography such as ground/soil conditions, the amount of sunlight and wind received, and variances in segment configuration
  - Such variances likely necessitate individual segment testing to provide reasonable assurance of adequate protection for the NRC to have confidence in DMA's ability to fulfill the detection and assessment functions

Defense in Depth

- Single act can eliminate sensor as point of failure
- → However, could this act as detection?
- Then, how to assess attack direction after elimination of sensor
- Redundancy of assessment