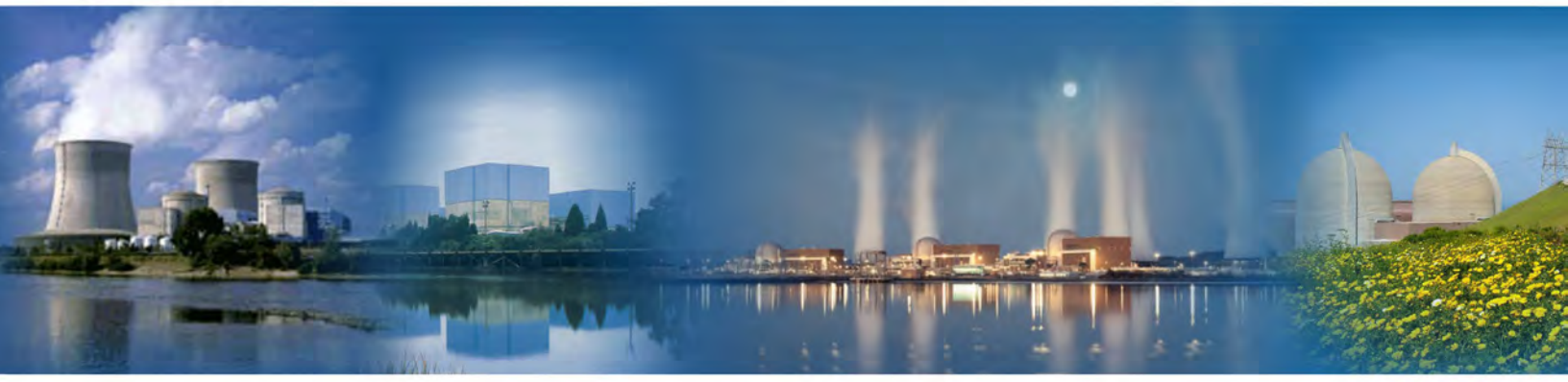
SAND2025-11386R

Light Water Reactor Sustainability Program
Plan for the Vulnerability Analysis of Deliberate Motion Analytics Algorithm



September 2025

U.S. Department of Energy
Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

This page left blank

SAND2025-11386R

Plan for the Vulnerability Analysis of Deliberate Motion Analytics Algorithm

John “JR” Russell

September 2025

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

This page left blank

ACKNOWLEDGEMENTS

The authors wish to acknowledge the support of the Department of Energy's Office of Nuclear Energy for funding the development of the Deliberate Motion Analytics Algorithm.
Their support has led to the creation of a new instantiation of artificial intelligence that can be applied to intrusion detection sensors that is expected to be an enabling technology for future security. It has led to new security designs that perform better than traditional systems at a fraction of the cost.

This page left blank

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
CFR	Code of Federal Regulations
COTS	commercial-off-the-shelf
CUI	Controlled Unclassified Information
DMA	deliberate motion analytics
DOE	Department of Energy
DOE-NE	Department of Energy, Office of Nuclear Energy
ES&H	Environment Safety and Health
FLEX	Diverse and Flexible Mitigation Capability
FY	fiscal year
LiDAR	light detection and ranging
LWRS	Light Water Reactor Sustainability
NAR	nuisance alarm rate
NEPA	National Environmental Policy Act
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
QA	quality assurance
R&D	research and development
RMF	Risk Management Framework
Sandia	Sandia National Laboratories
SNM	special nuclear material
SNSI	Secret National Security Information
U.S.	United States

This page left blank

1. INTRODUCTION

With the support from the Department of Energy's Office of Nuclear Energy (DOE-NE), Sandia National Labs partnered with Management Sciences Inc. (MSI) to develop an intrusion detection algorithm called the Deliberate Motion Analytics algorithm (DMA). DMA is capable of fusing data from commercial-off-the-shelf (COTS) sensors to enhance intruder detection and reduce nuisance alarms. The DMA algorithm has been tested in the following security environments:

- Two Fence Perimeters [11]
- Beyond the Fence [12][13][14]
- Water Intake[1]
- Drone Detection [15]
- Land Water Interface (dynamic shoreline) [16]
- Simulated Small Modular Reactor [12]

In all cases, except the Water Intake test results[1], the DMA based sensor system demonstrated improved intruder detection and reduced nuisance alarms. In July 2024, the results of the tests were discussed with the Nuclear Regulatory Commission (NRC) [17]. One of the outcomes from the discussion with NRC was that they would like to see a vulnerability assessment of the DMA algorithm to determine if there are any unacceptable vulnerabilities not revealed during the previous tests.

The purpose of this document is to provide a high-level test plan for the vulnerability assessment of the DMA algorithm, scheduled to be conducted in fiscal year (FY) 2026. A testbed will be created at Sandia's Sensor Technology Evaluation Center (STEC). Aerial views of the testbed are shown in Figure 3-1, Figure 3-2, and Figure 3-3.

The planned vulnerability assessment will consist of multiple evaluations from different agencies with the intent of passing thru a DMA detection zone without being detected. Vulnerabilities demonstrated will be studied to determine if the vulnerability was due to a sensor(s) limitation or a limitation of the DMA algorithm. This is an important clarification to understand.

Because of the way the DMA algorithm functions, it may be demonstrated that a sensor vulnerability does exist, but because of DMA's spatial and temporal sensor fusion of complementary sensors [20], the DMA intrusion detection system will still detect the simulated intruder and individual sensor limitations will not be manifested. A brief description of the DMA algorithm is provided in Appendix E

[1] The results for the Water Intake testing were in progress at the time this document was written, consequently the final results were not available.

This page left blank

2. BACKGROUND ON THE LIGHT WATER REACTOR SUSTAINABILITY PROGRAM

In FY 2019, the United Stated (U.S.) DOE-NE Light Water Reactor Sustainability (LWRS) program developed the Physical Security Pathway program with research aims to create tools, technologies, and risk-informed physical security decisions and activities with the following three research thrust areas:

1. **Advanced Security Technologies –** Provide an economic and technical evaluation of remote weapon technology, develop the final denial system technical basis necessary to implement components within the system, and develop an implementation basis for installation of a remote weapons platform at a nuclear utility site that meets regulatory requirements for inclusion in their security posture. This will enable the utility to optimize and enhance their security posture. The research is intended to support a cooperative private-public implementation of the technical basis at a candidate nuclear utility site with a candidate final denial system.
2. **Risk-Informed Physical Security –** Enhance, develop, and demonstrate risk-informed technologies for physical security by integrating dynamic risk methods, physics-based modeling and simulation, operator actions, and Diverse and Flexible Mitigation Capability (FLEX) equipment, which should extend the adversarial timeline for response force success. This will also include exploring the expansion of existing risk-informed methods for nuclear security. The risk tools will enable commercial utilities to incorporate increased realism in their force-on-force models, take credit for operator actions and FLEX equipment, and move toward greater use of quantitative measures of performance in security posture and the technical basis for physical security at nuclear power plants (NPPs). The intent of this research is to use risk-informed methods and tools that enable utilities to optimize their physical security posture and demonstrate the updated physical security posture is as effective as before the change. Additionally, this thrust area will include working with stakeholders to evaluate the risks related to unattended openings that potentially are person-passable for duct work and piping openings, which is an identified gap in the technical basis for security pathways into a nuclear facility.
3. **Advanced Security Sensors and Barriers –** Develop low-cost, rapidly deployable detection and assessment technologies that could be applied to piping, walls, doors, perimeters, water inlets/outlets, and like facility components at nuclear utility sites. An enabling technology that can be used to create the system is technical embroidery, which is an emerging technology that can attach wire, fiber optics, and tubes to various substrate materials. The proposed work will explore advances in sensor and barrier technologies, including available COTS sensors for use in security applications. Where technology has not been developed to support the security needs, research and development (R&D) will be performed to increase advancements in the sensors and barrier systems. The vulnerability assessment of the DMA algorithm relates to Research Thrust Area 3, because it applies to developing and integrating technologies to provide synergistic results related to the detection of intruders at site boundaries.

2.1. LWRS Motivation

Domestic nuclear power generation faces increasing economic pressures, in part from post-Fukushima regulatory requirements, an increase in subsidized renewable energy sources, and

current low-cost natural gas. The requirement for U.S. nuclear power generation sites, post-9/11, to maintain a large onsite physical security program is a key factor in high plant operational costs. U.S. NPPs are seeking novel physical security methods and technologies to help deliver on the "Nuclear Promise" [1].

The Department of Energy (DOE) national laboratories have extensively studied physical security configurations that couple detect, delay, and response attributes to regulatory-required physical security postures. This DOE-NE LWRS Program research pathway seeks to create tools, methods, and technologies that will accomplish the following:

- Apply aspects of risk-informed techniques for physical security decisions and activities to account for a dynamic adversary
- Apply advanced modeling and simulation tools to better inform physical security posture
- Assess benefits from proposed enhancements, novel mitigation strategies, and potential changes to regulatory guidance
- Enhance the technical basis necessary for operating utilities to reevaluate their physical security posture while meeting regulatory requirements

2.2. LWRS Purpose and Goals

The following are the primary deliverables for the Physical Security Pathway:

- Provide validated methods and justifications that can be used to implement an updated physical security regime and optimize the physical security at domestic NPPs
- Develop tools that create a robust risk-informed technical basis for physical security decisions
- Create potential security architectures that incorporate technology to optimize human-in-the-loop activities
- Implement results of this initiative into national consensus standards

The intent of the DOE-NE LWRS Physical Security Pathway is to develop methods, tools, and technologies and generate recommendations that provide the technical basis for an optimized plant security posture. This could include considering reducing conservatisms in that posture to decrease security costs for the nuclear industry, while still ensuring adequate physical security.

The Physical Security Pathway R&D activities will analyze the existing physical security regime (e.g., regulations, personnel, technologies) and current best fleet practices to compare and contrast insights derived from this activity with alternatives and methods that leverage advanced modeling and simulation, modern technologies, and other advanced techniques to enhance approaches for domestic NPP physical security.

All activities in this physical security initiative will be performed in accordance with the DOE-NE LWRS Program's quality assurance (QA) plan. Appropriate QA rigor will be applied for the intended use of the data. An appropriate export control and classification review will be performed to ensure that the milestone deliverables are uploaded to DOE Office of Scientific and Technical Information, when applicable. Any sensitive information generated by this initiative will be handled in accordance with established DOE requirements.

2.3. Regulatory Requirements

Code of Federal Regulations (CFR) 10 CFR 73, "Physical Protection of Plants and Materials," [2] prescribes requirements for the establishment and maintenance of a physical protection system that will have capabilities for the protection of special nuclear material (SNM) at fixed sites and in transit and for NPPs in which SNM is used. 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," [3] requires each nuclear power reactor licensee to implement the requirements of 10 CFR 73.55 through its U.S. NRC-approved physical security plan, training and qualification plan, safeguards contingency plan, and cybersecurity plan, which will be referred to collectively hereafter as security plans.

The requirements of 10 CFR 73.55 are intended to establish and maintain a physical protection program that provides reasonable assurance that activities involving SNM are not contrary to common defense and security and do not constitute an unreasonable risk to public health and safety. This includes the ability to protect against the design basis threat of radiological sabotage (i.e., significant core damage and spent fuel sabotage). The security plans describe how the 10 CFR 73.55 requirements will be implemented through the establishment and maintenance of a security organization, use of security equipment and technology, training and qualification of security personnel, implementation of predetermined response plans and strategies, and protection of digital computer and communication systems and networks.

2.3.1. Physical Security Requirements

The nuclear power reactor licensee is responsible for maintaining the onsite physical protection program in accordance with NRC regulations through the implementation of security plans and written security-implementing procedures. The design of the physical protection program is focused on a series of target sets that require protection. A critical element of the security plan is demonstrating the ability to meet requirements, including the capability of armed and unarmed personnel to perform assigned duties and responsibilities outlined in the security plans and procedures. That leads to the development and implementation of a training and qualification program (in accordance with 10 CFR 73.55, Appendix B, Section VI) and a performance evaluation program (10 CFR 73.55, Appendix B) to ensure the effectiveness of the licensee's armed and unarmed personnel.

2.3.2. Additional Security Requirements

In addition to the physical security requirements, the licensee's security plans include details describing the following related security topics:

- The requirements for the access authorization program as stipulated in 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants" [4].
- A Safeguards Contingency Plan that describes how the criteria set forth in 10 CFR 73.5, Appendix C, Section II, "Licensee Safeguards Contingency Plans," of which Part 73 will be implemented [5].
- A Cybersecurity plan that describes how the criteria set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," will be implemented [6].
- Regulatory Guide 5.44 [18] requires detection of penetration or attempted penetration of the protected area. The design goal of a perimeter intrusion detection system is to detect an individual weighing a minimum of 35 kg (77 pounds), whether the individual is running, walking, crawling, jumping, or rolling through the perimeter of a protected area. The design

goal of a perimeter intrusion detection system should be to limit false alarms and nuisance alarms to no more than one false alarm per zone per day and one nuisance alarm per zone per day.

- It is difficult of find 77-pound intruders, so the simulated intruders used during performance testing will be larger.
- Walkers and runners will be included in the test matrix for performance testing.
- A 12-inch aluminum sphere radar target, which is estimated to have a radar cross section of .07 square meters, will be used to simulate crawlers. It is estimated that a hands and knees crawler will have a radar cross section of .3 square meters and a belly crawler has a .1 square meter radar cross section, so the 12-inch aluminum sphere is a conservative representation of a crawler [19].
- The tests conducted will be in a 40-meter-wide detection zone. An intruder jumping or rolling will create a larger radar cross section than the .07 square meter radar cross section presented by the 12-inch radar target, so the radar sphere represents a conservative representation of a jumper or a roller. Since the detection zone is 40 meters wide and the sensor's field of view spans the full 40 meters, it does not make sense to attempt to jump over the sensor's detection zone.
- In view of these estimates, jumpers and rollers will not be included in the test matrix for the performance testing and will be replaced by tests dragging the 12-inch aluminum sphere. Figure 2-1 and Figure 2-2 show images of the 12-inch aluminum sphere.

Figure 2-1. Image of the 12-inch aluminum sphere during testing

Figure 2-2. 12-inch aluminum sphere

2.3.3. How to Quantify Performance of an Intrusion Detection System

To be able to quantify an intrusion detection sensor, two metrics are required. They are the sensor's true positive and false positive performance. The true positive performance is quantified by the probability of sensing divided by the confidence level, and the false positive performance is quantified by nuisance alarm rate (NAR) measured in nuisance alarms per 24-hour period.
A nuisance alarm is any alarm declared by the sensor that is not caused by an intruder.
A vulnerability of a DMA base intrusion detection system will be reflected in the true positive test results.

3. PROJECT SCOPE AND TASKS

The ultimate goal of this effort is to determine if there are vulnerabilities in the DMA algorithm that an intruder could exploit to penetrate a DMA based intrusion detection system without being detected. The following sections describe the scope of the vulnerability tests and outlines the series of tasks that will be conducted to perform the vulnerability analysis of DMA.

3.1. Scope of the DMA Vulnerability Assessment

At the time this plan was written, the majority of the DMA code was in a development state, and not ready for a Cyber Vulnerability Analysis. The work so far has focused on demonstrating the physical intrusion detection performance of a DMA based intrusion detection system when deployed in various operational or operationally relevant environments. Tests were conducted using simulated intruders attempting to pass thru a DMA/sensor detection zone. Performance of the DMA/sensor system was quantified in terms of true positive and false positive results, described in Section 2.3, when subjected to a design basis threat[2].

At the time this plan was written, the DMA software (or code) was written in Python[3], which is a development code. Current plans in FY 2026 are to migrate DMA's Python software to a code that is more robust, such as C++ or Rust, and apply the National Institute of Standards and Technology's Risk Management Framework (RMF)[4]. After the updated DMA code has gone thru the RMF process, it will be ready for a cyber vulnerability analysis. Just prior to the time this plan was written, the DMA team was notified of DOE's intent to provide funding in FY 2026 to commercialize the DMA algorithm, which includes migrating it to a more robust software and applying the National Institute of Standards and Technology's RMF process.

Because the DMA code is not ready for a cyber vulnerability assessment, this effort will focus on the physical vulnerability assessment of the DMA.

3.2. Tasks Planned to Conduct the DMA Vulnerability Assessment

The following describes the high-level list of tasks needed to conduct the vulnerability assessment of the DMA algorithm followed by a more detailed description of each task.

4. Preliminary Preparations
5. Create Testbed
6. Conduct Base Line Tests
7. Conduct Internal Vulnerability Tests
8. Assemble and Invite Multidisciplinary Team/Multi-Agency Team to Participate

---

[2] For ground intruders the DBT consists of walkers, runners, crawlers, jumpers, and rollers.

[3] Python is a high-level, general-purpose programming language used by many developer because of its ease to quickly create a functioning code. Python is an interpreted language, meaning code is executed line by line rather than being compiled into machine code before execution.

[4] The NIST Risk Management Framework provides a structured, technology-agnostic process for managing cybersecurity, privacy, and supply chain risks throughout an information system's entire lifecycle, from preparation and ongoing monitoring to assessment and risk response. It helps federal agencies and private sector organizations to integrate risk management activities, select appropriate controls, and ensure that security and privacy are considered from the initial stages of development.
https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

9. Conduct Multi-Agency Vulnerability Tests
10. Write Report (Controlled Unclassified Information [CUI] report and possibly a Secret National Security Information [SNSI] appendix)
11. Brief Results (CUI Slides and possible SNSI Slides separately)

3.2.1. Preliminary Preparations

The preliminary preparations will include the following tasks that will address the National Environmental Policy Act (NEPA), Environment Safety and Health (ES&H), and Classification aspects of this activity.

- DOE requires NEPA approval for all projects. The paperwork for NEPA approval will be completed and submitted in the first few weeks of FY 2026.
- A review of the execution of the vulnerability tests will be reviewed with an ES&H subject matter expert early in FY 2026. A minor ES&H aspect of this work will be to address members from other agencies conducting tests. The DMA team will establish safety procedures and briefings for non-Sandians who will conduct tests in the testbed. Other ES&H documentation will be identified and completed.
- The classification of the results and subsequent documentation of the vulnerability tests will be discussed with Sandia's Classification Office early in FY 2026. It is expected that the Classification Guide for Safeguards and Security (CG-SS-5) will apply to the information resulting from the vulnerability study. It is anticipated that the final report will consist of a CUI document with a classified appendix.
- Another classification issue to address will be if there are DMA algorithm vulnerabilities that can be remedied by changes in the DMA software and how will the small company that wrote the code (they do not have clearances) make the changes. This issue will be discussed with DOE's/Sandia's Classification Office early in FY 2026.

3.2.2. Create Test Bed

A testbed will be created to detect ground intruders in an "un-engineered" environment, with the intent of detecting ground intruders, as opposed to drone detection or swimmer detection. Ground intrusion scenarios were selected instead of drone or swimmer scenarios, because ground intrusions will be easier to conduct and will still provide a valid basis for the vulnerability assessment of the DMA algorithm.

The testbed will be located at Sandia's Sensor Technology Evaluation Center. The term "un-engineered" implies that the testbed will not be graded or leveled, and the layer of small rock normally used to cover the clear zone in the two fence perimeters will not spread over the testbed. The foliage will be mowed to a height of 3–6 inches tall. Figure 3-1, Figure 3-2, and Figure 3-3 show an aerial views of the proposed testbed, sensor locations, sensor's field of view, and proposed test area for the vulnerability tests. The "Proposed Test Area for Vulnerability Testing," show in Figure 3-3 is also where the baseline tests will be conducted (Section 3.2.3) and nuisance alarm data will be recorded.

Current plans for the testbed are to deploy radar, LiDAR, and thermal imagers with video analytics. The sensor outputs will be fused temporally and spatially to form DMA tracks. The DMA tracks will be analyzed to determine the presence of deliberate motion in order to declare an alarm. The following sensors will be used:

- Radar: the FLIR R1 Radar
- LiDAR: the Aeries II, Aeva LiDAR
- Thermal Imager/Video Analytics: the FLIR DX-650 Imager with Evolon Video Analytics

Normal camera coverage will also be provided to enable general awareness of activities during testing using the DX-650. It has pan, tilt, and zoom capabilities for both thermal and visible imagery. Appendix A through Appendix D provide specifications of each sensor technology described above.

Figure 3-1. Aerial view of the testbed

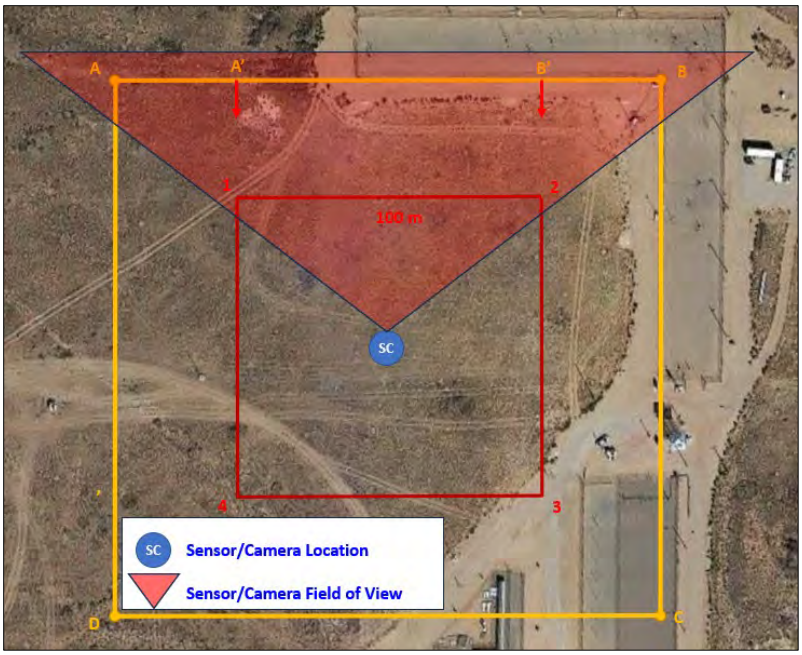


Figure 3-2. Testbed showing sensor location and sensor field of view

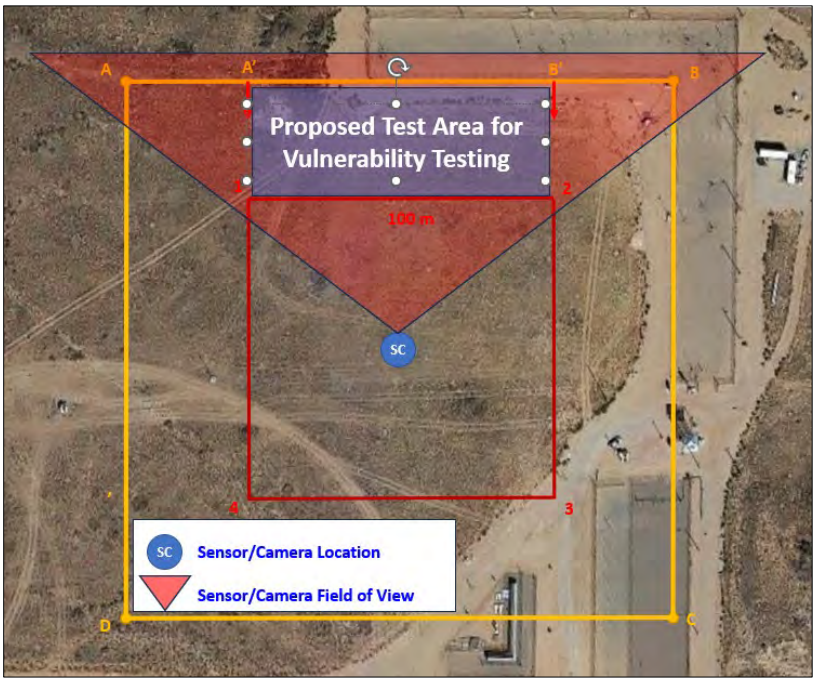


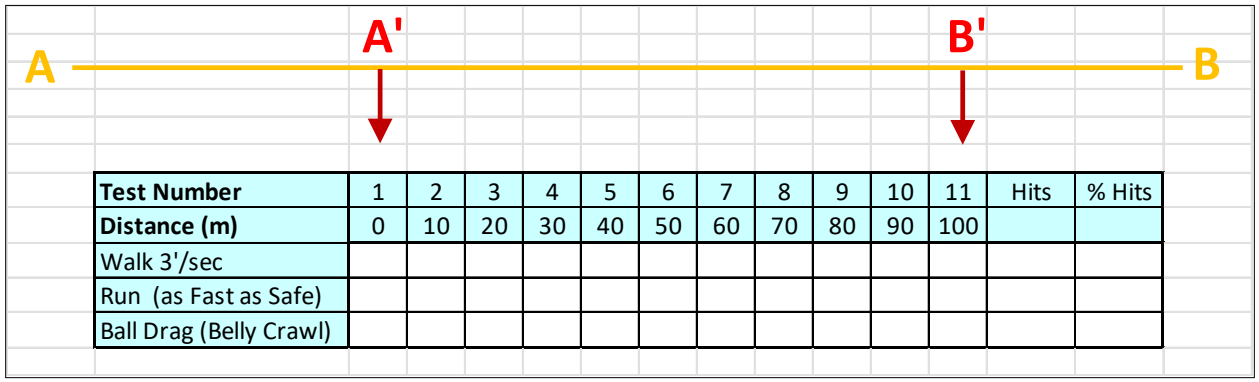
Figure 3-3. Testbed showing proposed test area for vulnerability testing

3.2.3. Conduct Base Line Tests

A set of baseline tests will be conducted to verify the sensors and the algorithm are functioning properly. The simulated intrusion tests will include walkers, runners, and a 12-inch aluminum radar target to simulate crawlers, jumpers, and rollers. The baseline tests will be conducted in the "Proposed Test Area for Vulnerability Tests" shown in Figure 3-3. A test matrix showing the baseline tests is shown in Table 3-1. The test paths are depicted in Figure 3-4. If a more rigorous

performance test was desired, 30 or more tests would be conducted and limited statistics could be established, as described in Section 2.3.3. Since the intent of the baseline tests are to show that the sensors and algorithm are functioning properly, a full set of 30 or more tests will not be conducted. After the simulated intrusions are conducted, nuisance alarm data will be recorded an analyzed. The simulated intrusions data and the nuisance alarm data will constitute the basis for the baseline testing. After completing this task, the vulnerability test will begin.

Table 3-1. Test matrix for baseline tests



Test Number	1	2	3	4	5	6	7	8	9	10	11	Hits	% Hits
Distance (m)	0	10	20	30	40	50	60	70	80	90	100		
Walk 3'/sec													
Run (as Fast as Safe)													
Ball Drag (Belly Crawl)													

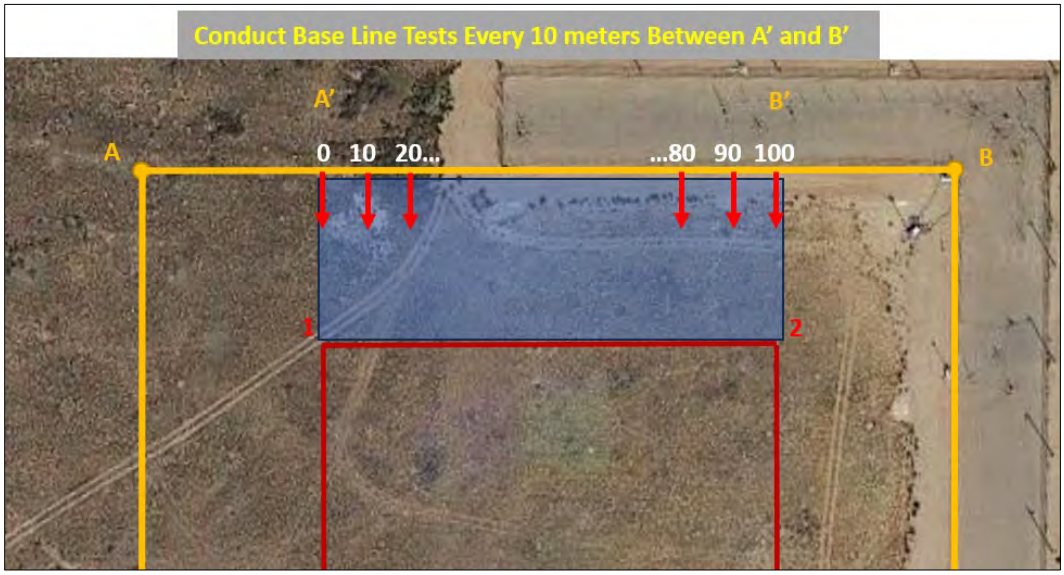


Figure 3-4. Testbed showing test paths for baseline testing

3.2.4. Conduct Internal Vulnerability Tests

A multidisciplinary team will be created that will including Sandia security subject matter experts and the DMA algorithm developers. The team will perform a preliminary set of vulnerability tests. The preparation for the vulnerability activity will consist of a description of the sensor technologies deployed in the testbed and a description of the DMA algorithm. After describing the sensor technologies and algorithm, a brainstorming discussion will be held to generate ideas for attack vectors and spoofing techniques to try in the testbed. The results will be recorded after each test and videos of the simulated attack will be recorded as well. It is expected that multiple iterations of the

brainstorming/testing process will occur. The proposed process can be summarized in the following three steps.

1. Brief team on sensor technologies and DMA algorithm
2. Conduct brainstorming session to generate possible attack strategies
3. Conduct and record tests

Analysis of the outcomes from the vulnerability tests may identify corrections to the algorithm. If changes to the DMA software completed, another set of baseline tests will need to be conducted to ensure changes in the algorithm do not result in degradation of the detection and nuisance alarm performance.

3.2.5. Assemble and Invite a Multidisciplinary Team/Multiagency Team to Participate

Assembling and inviting a multidisciplinary and multiagency team will be a key task for this activity. The purpose of inviting multiple agencies to participate in this activity is to insure that multiple perspectives are brought to identify any vulnerabilities of the DMA algorithm. The DMA team will send out invitations to multiple groups with a proposed schedule to allow personnel that want to participate time to travel. Currently, the following groups will be invited:

- NRC Security Specialists (must have)
- Security specialists from Sandia (nice to have)
- DOE's Composite Adversary Team (nice to have)
- Department of Defense's Joint Ember Immune Team (nice to have)
- Members from other national labs (nice to have)

In the list above, having the NRC security specialists participate in this study is critical. This study is being conducted because of their request during briefings on DMA. It would be great to get input from the other agencies/personnel, but NRC participation is the most important.

3.2.6. Conduct Multi-Agency Vulnerability Tests

It is expected that the multi-agency vulnerability test will be conducted within a one-month period. The current plans are to conduct these tests during March or April of 2026. The dates that these tests may actually occur may vary, because the funding outlook and budgets for travel for many agencies is uncertain at the time this document was written. The funding issue may limit the ability of other agency personnel to travel to Sandia to participate.

One way to mitigate the funding/travel issue is to set up video conferences to discuss possible attack strategies with other agency personnel that will then be conducted by the DMA team. It would be optimal to allow personnel to conduct their own proposed attacks, but the video conference strategy does allow the effort to capture a broader set of approaches and ideas that may reveal vulnerabilities.

If the multi-agency personnel are present to conduct vulnerability tests, the same process described in Section 3.2.4 will be followed.

1. Brief team on sensor technologies and DMA algorithm
2. Conduct brainstorming session to generate possible attack strategies
3. Conduct and record tests

As described in Section 3.2.4, several iterations of the three-step process may occur. All tests conducted will be recorded. The tests conducted will not be classified. When in the field, tests will

be recorded in the terms Test 1, 2, 3, etc. The results will be described as detected/not detected. The tally of test numbers and results will not be classified. When the description of what constitutes Test 1, 2, 3, etc. is added to the detect/no detect results, that aggregate information may be classified. This strategy to address classified information in the field will be discussed with the DOE/Sandia Classification Office.

After the multi-agency tests are concluded, an out brief to the team will be given. The test results will be summarized, and the classification of the results will be given. The attack team members will be asked not to discuss the results in an unclassified environment or pass on classified information in channels not appropriate classified information.

3.2.7. Write Report (CUI report and possibly an SNSI appendix)

Documenting the results of the vulnerability assessment will take between 2–6 weeks. If there are classified sections, writing the classified materials will take longer than the unclassified. The current plan is to write the majority of the report in an unclassified environment at the CUI level. If there are vulnerabilities, they will likely be classified SNSI following the classification guidance in DOE's CG-SS-5 (Classification Guidance – Safeguards and Security -5). A classified appendix written on the appropriate network to process classified material will be referenced in the unclassified body of the report.

Another classification issue needing to be addressed is if there are DMA algorithm vulnerabilities that can be remedied by changes in the DMA software, how does the small company (MSI) that wrote the code make the changes. MSI does not have clearances. This issue will be discussed with DOE's/Sandia's Classification Office early in FY 2026.

3.2.8. Brief Results (CUI Slides and possible SNSI Slides separate)

Similar to the report, the majority of the slides will be CUI. If there are vulnerabilities that are deemed to be SNSI, they will be created on a separate system certified to process classified information at the SNSI level.

If presentations are given outside of Sandia's Limited Area or at other agencies, the classified slides will be sent thru the appropriate channels.

REFERENCES

[1] Nuclear Energy Institute, "Delivering the Nuclear Promise," 2016-2019 https://www.nei.org/resources/delivering-the-nuclear-promise

[2] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73. "Physical Protection of Plants and Materials." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/

[3] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 55. "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html

[4] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 56. "Personnel Access Authorization Requirements for Nuclear Power Plants." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0056.html

[5] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Appendix C Section II. "Licensee Safeguards Contingency Plans." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-appc.html

[6] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 54. "Protection of Digital Computer and Communication Systems and Networks." https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html

[7] "Available Patents & Technologies | Stevens Institute of Technology." n.d. Techpublisher.stevens.edu. Accessed September 14, 2022. https://techpublisher.stevens.edu/tech/Passive_Underwater_Acoustic_System_For_Detection

[8] Bruno, Michael, Barry Bunin, Laurent Fillinger, Howard Goheen, Alexander Sedunov, Nikolay Sedunov, Alexander Sutin, et al. n.d. "Passive Acoustic Underwater Intruder Detection System." Accessed September 14, 2022. https://www.freepatentsonline.com/8195409.html.

[9] Russell, John, Diego Molina, Cosmic Narvaiz, Andrew Danilich, "Preliminary Study of Detection of Swimmers at Water Intakes for Nuclear Power Plants: Update," March 2024, SAND2024-04492R.

[10] Cooke, J., et. al., "Binomial Reliability Table (Lower Confidence Limits for the Binomial Distribution)", U.S. Naval Ordnance Test Station, NAVWEPS Report 8090, January 1964.

[11] Russell, J., C. Stern, P. Blemel, D. Molina, C. Narvaiz, A. Danilich, "Pilot Deployment of Deliberate Motion Analytics Sensor System at the Monticello Nuclear Power Plant," SAND2024-00834R, Sandia National Laboratories, Albuquerque, NM, January 2024

[12] Russell, J., C. Stern, P. Blemel, D. Molina, C. Narvaiz, A. Danilich, "Multi-Sector, Multi-Intruder Test Results for DMA enabled PIDS (DPIDS)," SAND2024-01437R, Sandia National Laboratories, Albuquerque, NM, January 2024

[13] Russell, J., C. Stern, P. Blemel, and A. Woo, "Deliberate Motion Analytics Fused Radar and Video Test Results – Deployed Beyond the Perimeter Fence in a High Noise Environment," SAND2021-5413, Sandia National Laboratories, Albuquerque, NM, April 2021.

[14] Russell, J., C. Stern, P. Blemel, D. Molina, A. Garcia, "Pilot Deployment of the Deliberate Motion Analytic Sensor System at Waterford III Nuclear Power Plant," SAND 2022-14815R, Sandia National Laboratories, Albuquerque, NM, September 2022.

[15] Russell, J., C. Stern, P. Blemel, D. Molina, "Enhanced Unmanned Aerial System Using Sensor Fusion and Deliberate Motion Algorithms," SAND 2023-06871R, Sandia National Laboratories, Albuquerque, NM, September 2022.

[16] Russell, J., C. Stern, P. Blemel, D. Molina, D. Dominguez, "Pilot Deployment of the Deliberate Motion Analytic Sensor System at the Donald C. Cook Nuclear Plant," SAND 2022-07758, Sandia National Laboratories, Albuquerque, NM, June 2022.

[17] Russell, J., "Summary of DMA Technical Exchange with the Nuclear Regulatory Commission," SAND 2024-10300R, Sandia National Laboratories, Albuquerque, NM, August 2024.

[18] United States Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Regulatory Guide 5.44, Revision 3, "Perimeter Intrusion Alarm Systems."

[19] https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/PB97926902.xhtml

[20] Russell, J., D. Lee, J. Bonilla, D. Molina, D. Osborn, "Microwave Sensor Performance at "Slow" Setting and Alternate Stainless Steel Test Target for Microwaves," SAND2022-15618R, Sandia National Laboratories, Albuquerque, NM, November 2022

[21] Russell, J., "Complementary Sensor Selection for High Security Applications," presented to the International Nuclear Materials Management Conference (September 2012).

APPENDIX A. SPECIFICATIONS OF THE FLIR R1 RADAR

FLIR

SHORT-RANGE PERIMETER SURVEILLANCE RADAR

FLIR Ranger® R1

The FLIR Ranger® R1 is a ground-based perimeter surveillance and tracking radar that accurately detects personnel and vehicles at a range of up to 700 m. It scans a full 360° every second, covering up to 1.5 square km (0.6 square miles). Additional units – such as a mid-range FLIR Ranger® R2 – can be networked in an overlapping array to protect larger areas, stitching together an impassable radar area outside and inside your perimeter.

Operating in the Ka-band, this radar is compact and highly portable. It works in virtually any climate, weather, or lighting condition, providing 24/7 security. R1 is ideal for force protection and securing borders, airports, seaports, and critical infrastructure. R1 provides fast and accurate detection of up to 128 threats simultaneously. Ethernet XML target data in GIS coordinates, as well as wireless and fiber connectivity, makes R1 integration a snap.

FEATURES

ADD RADARS FOR WIDER COVERAGE
Network multiple units with the full range of FLIR radars and imagers to cover terrain profiles inside and outside perimeters.

LOW FALSE ALARM RATE
Accuracy, ease of operation, and the lowest false alarm rate in the industry, separates FLIR Ranger radars from the competition.

THE POWER OF RADAR + IMAGING
Using the radar's advantage in continuously detecting multiple targets allows linked thermal and EO cameras to focus on quickly classifying each threat.

FAST, ACCURATE THREAT DETECTION
R1 quickly detects up to 128 threats simultaneously while accurately displaying each target's location.

RELIABLE OPERATION & EASY INTEGRATION
High availability rate saves on costs for spare systems or repairs, and it requires only one cable and four bolts for integration.

APPLICATIONS

SECURE BORDERS

MONITOR PORTS

GUARD INDUSTRIAL FACILITIES

FORCE PROTECTION

DEFEND PUBLIC INFRASTRUCTURE

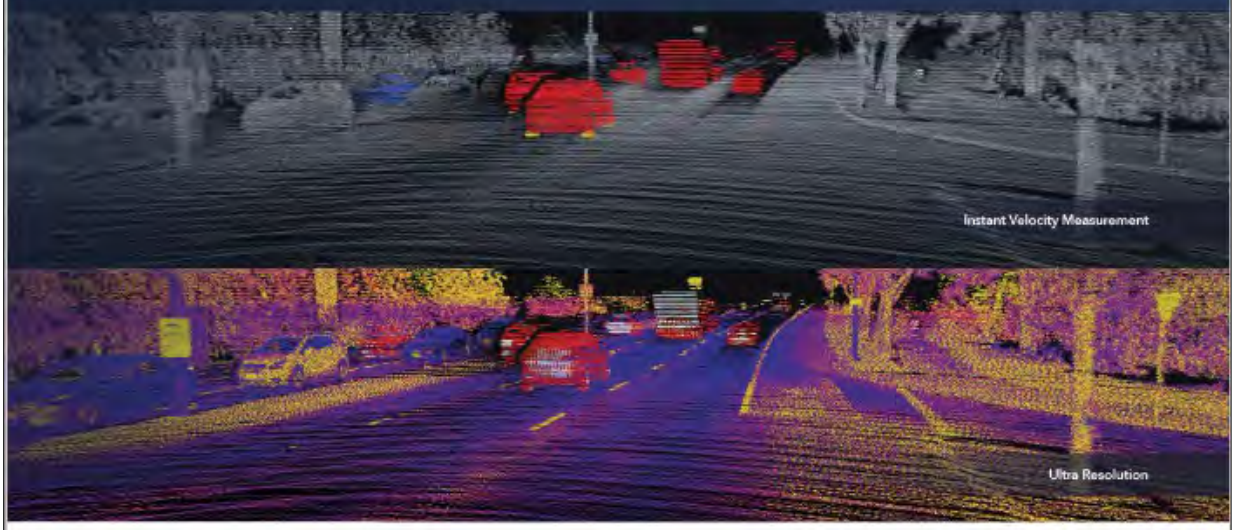
General Specifications

Ranger R1	
Frequency	Ka band
Resolution	0.3 m range, 1° azimuth
Scan Rate	1 rev/sec (60 rpm)
Beam Width	Azimuth 1° (2-way) Elevation 6° (2-way)
Target Type	Moving vehicles & personnel
Target Velocity	0.1 m/s to 50 m/s
Data Output	Lat./Long. or Range/Angle
Data Bandwidth	Min: 1 Mbits without PPI - Max: 7 Mbit with PPI
Communications	Ethernet, wireless, fiber
Protocol	ICD 0100
XML	Yes
Network	8 per server; total unlimited
Input Power	20 to 32 VDC, 24 VDC nominal
Power Consumption	45 watts
Environmental	NEMA 4
Temperature	Operating: -30°C to +65°C Storage: -40°C to +70°C
Humidity	50% ± 5 to 95% ± 4 Non-condensing (60°C max)
Altitude	Up to 15,000 ft (operating and storage)
Wind	Up to 120 km/hr
Shock	40 g peak for 20 ms, half sine (with vibration mount)
Vibration	MIL-STD-810F
Ratings	FCC Class B, EN 301480, Parts 1 & 3; CE: EN 60215 EN 3000 19-1 (Class 4.1E) EN 300019-1-5 (Class 5.2, Including mechanical class 5M3)
Size	14.4" height x 18.25" diameter (364 x 461mm)
Weight	29 lbs (13.1 Kg)
Range	
Operating Range	5 – 700 m
Target	Walking 5 – 700 m Running 5 – 700 m Hands/Knees 5 – 500 m Low Crawl 5 – 500 m Swimming 5 – 500 m
Target Detection (Vehicles & Watercraft)	5 – 700 m
Coverage Area	1.54 km^2 (0.60 mi^2)
Mask Zones	Two selectable angular blank sectors. Unlimited Polygon detection zones.
Options	
Camera integration	
Networkable - up to 8 units per server	
Wireless Ethernet Communication	
Fiber optic communications	
Vibration mount	

APPENDIX B. SPECIFICATIONS OF THE AEVA LIDAR

AERIES™ II

World's First 4D LiDAR™ with Camera Level Resolution



Aeries II is the world's first 4D LiDAR sensor with unparalleled capabilities built from the ground up to enable the next generation of autonomy.

Leveraging Aeva's unique Frequency Modulated Continuous Wave (FMCW) 4D technology and the world's first LiDAR on chip design, the sensor's capabilities go beyond legacy LiDAR, allowing it to detect instantaneous velocity for every pixel in addition to 3D position, with camera-level Ultra Resolution™.

KEY FEATURES

- **Automotive Reliability**
- **LiDAR-on-Chip**
- **Instant Velocity Detection**
- **Compact Design**
- **Multiple FoVs**
- **Free From All Interference**
- **Ultra Long Range**

4D PERCEPTION HIGHLIGHTS

Ultra Resolution
Real-time camera-level resolution up to 1000 lines for static world

Long Range Dynamic Object Detection & Tracking
Detection and tracking for dynamic objects up to 500 meters

Centimeter Precision Vehicle State Estimation
6-DoF vehicle state estimation in GNSS denied environments without external sensors

Automotive Grade Reliability

Designed, tested and certified for reliability with automotive-grade ratings for ingress, impact, and shock and vibration to ensure peak performance across a variety of vehicle class, road and environmental conditions. The compact design allows for a wide range of sensor placements in automotive and non-automotive applications, with multiple on-the-fly, software configurable FoV, scan pattern and maximum range options.

SENSOR PERFORMANCE

Configuration	Wide FoV	Medium FoV	Narrow FoV
Maximum Horizontal Field of View	120°	55°	35°
Nominal Lines per Frame	80	140	200
Maximum Range	500m	500m	500m
Range for 10% Reflectivity	Up to 200m	Up to 200m	Up to 200m
Frame Rate	Up to 20Hz	Up to 20Hz	Up to 20Hz
Minimum Angular Resolution	0.025° (H) x 0.025° (V)	0.025° (H) x 0.025° (V)	0.025° (H) x 0.025° (V)
Maximum Vertical Field of View	30°	30°	30°
Minimum Range Precision (1-σ)	2cm	2cm	2cm
Minimum Velocity Precision (1-σ)	3cm/s	3cm/s	3cm/s

MECHANICAL / ELECTRICAL

Dimensions	15 x 12 x 7cm
Weight	1.8 Kg
Interface	1000BASE-T1
Operating Voltage	9 - 18V

OPERATION / ENVIRONMENTAL

Operating Temperature	-40°C to 85°C
Laser Safety	Class 1
Reliability (Mechanical & Electrical)	ISO 16750, LV124
Ingress Rating	IP67
Impact Rating	IK07

DATA PRODUCTS

Sensor Output	Instant Velocity, Reflectivity, Position (X,Y,Z), Point Confidence
Software Tools	Aeviz® Visualization, API
Diagnostic	System Self Test, Blockage Detection
4D Perception Software	Ultra Resolution, Dynamic Object Detection and Tracking, Ego State Estimation, Real-time Horizon Tracking
Scene Segmentation	Road Markings, Drivable Regions, Vegetation, Barriers

INDUSTRY APPLICATIONS

Automotive | Trucking | Mobility | Industrial Automation | Smart Infrastructure | Warehouse Automation

APPENDIX C. SPECIFICATIONS OF THE EVOLON VIDEO ANALYTICS

Universally Applicable AI Classification

Evolon Enterprise features a groundbreaking combination of robust object detection married to advanced artificial intelligence-driven object classification that helps to ensure alerting on only valid threats. With Evolon Enterprise, organizations benefit from the latest edge-based, real-time detection of threats with over 90% fewer false alarms, all delivered by a universally applicable camera-agnostic solution.

Evolon Enterprise boasts a slew of enhancements and new features that significantly augment its capabilities and boost its value to users.

Key Features evolon Enterprise

- **Artificial Intelligence-driven Object Classification *NEW***
  Accurate and proactive detection and classification of objects and potential threats.
- **Active Scene Management® *NEW***
  Helps mitigate alerts caused by rain or insects attracted to camera IR.
- **True Detect *NEW***
  Cuts through the noise caused by light events such as reflected light, vehicle headlights and glare.
- **Dwell Detection *NEW***
  Monitor an area of interest for loitering that is supposed to be cleared of all activity and trigger an alarm.
- **Global Scheduler *NEW***
  Allows users to establish a universal schedule for all cameras on the server.
- **Instant Training *NEW***
  User interface includes a "Walkthrough" feature that provides instant training or a quick refresher.

Comprehensive object classification in any setting.

Accurate object detection, even in low light situations.

See through the storm, ignore alerts usually casused by natural phenomena.

Simplify security, decrease alerts caused by bugs and insects.

APPENDIX D. SPECIFICATIONS OF THE FLIR BI-SPECTRAL IMAGER, ELARA DX-SERIES

FLIR

MULTI-SPECTRAL PTZ CAMERA

FLIR Elara™ DX-Series

The FLIR Elara DX multi-spectral pan/tilt/zoom (PTZ) security camera provides full situational awareness in the most punishing environments. Combining thermal and visible light imagers, the Elara DX gives operators the ability to monitor large areas in complete darkness, glaring light, and adverse weather. The exceptional detection and identification capabilities of multi-spectral cameras help integrators provide high-quality solutions for challenging imaging problems at critical infrastructure sites and remote facilities.

www.flir.com/security

MULTI-SPECTRAL IMAGING IN ANY CONDITION

Integrated thermal and visible sensors capture sharp video where other PTZ cameras cannot.

- Thermal sensor provides complete awareness in rain, snow, light fog, and total darkness
- 4K visible resolution produces exceptional clarity
- Onboard IR illuminator enables excellent low light visible imaging
- Visible sensor optical zoom up to 31x

DESIGNED TO WITHSTAND EXTREME ENVIRONMENTS

Built to handle the challenges of critical infrastructure sites and other demanding locations.

- IP66- and NEMA-4X-rated
- Available lens wiper/washer keeps lenses clean and clear in remote installations
- Extreme operating temperature range of -40°C to 60°C
- Discreet pendant form factor

BUILT-IN, HIGH-QUALITY CYBERSECURITY HARDENING

Enhanced cybersecurity measures safeguard system from developing threats.

- Easy-to-use web interface simplifies set-up across all FLIR security cameras
- Regular firmware updates offer additional features and security improvements

SPECIFICATIONS

Thermal Sensor & Optics				
Array Format	640 x 480 & 320 x 240			
Thermal Sensitivity	< 50mK@ 25°C			
Detector Type	Long-Life, Uncooled VOx Microbolometer			
Pixel Pitch	12 µm			
Thermal Frame Rate	NTSC: 30 Hz or PAL: 25 Hz / 8.3 Hz			
Optical Characteristics	Model	FOV	Focal Length	F#
	DX-350	50° x 38°	4.3 mm	F/1.0
	DX-324	24° x 18°	9.1 mm	F/1.0
	DX-312	12° x 9°	18 mm	F/1.0
	DX-306	6° x 5°	36 mm	F/1.0
	DX-650	50° x 38°	8.7 mm	F/1.0
	DX-624	24° x 18°	18 mm	F/1.0
	DX-612	12° x 9°	36 mm	F/1.0
	DX-608	8° x 6°	55 mm	F/1.0
E-Zoom	Continuous E-Zoom to 4x			
Spectral Range	7.5 µm to 13.5 µm			
Focus Range	Athermalized, Focus-Free			
Video				
Video Compression	Thermal: One channel of H.264 & M-JPEG Visible: Two independent channels of H.264 & M-JPEG			
Streaming Resolution	Thermal: QVGA to VGA Visible: VGA to 4k			
Thermal Image Settings	Auto AGC, Dynamic Detail Enhancement (DDE), Brightness, Sharpness, Contrast			
Thermal AGC Region of Interest (ROI)	Default, Presets and User definable to ensure optimal image quality on subjects of interest			
Image Uniformity Optimization	Automatic Flat Field Correction (FFC) - Thermal and Temporal Triggers			
System Integration				
Ethernet	10/100/1000 Mbps			
Network APIs	FLIR SDK, FLIR CGI, ONVIF Profile S			
Digital I/O	Input: 4 Sets / 5V 10kΩ pull up Output: 2 Set / Relay output, max. 130mA 24VDC/AC			
Audio I/O	Bi-Directional Audio - connection - Terminal block			
Illumination	Up to 200m NIR illumination Distance: Up to 200m (656ft.) / 90° Peak emission wavelength: 850			
Wiper	Wiper is standard and camera is compatible with a washer accessory			
Network				
Supported Protocols	IPV4, HTTP, UPnP, DNS, NTP, RTSP, RTP, TCP, UDP, ICMP, IGMP, DHCP, ARP			
Pan / Tilt Performance				
Pan Angle / Speed	Continuous 360° - 0.1° to 90° /sec			
Tilt Angle / Speed	-10° to 190° - 0.1° to 60°/sec			
Programmable Presets	256			

General	
Input Voltage	24 VAC(±10%) Universal POE injector
Weight	9.1kg (20.1lb)
Dimensions	Diameter: 275mm (10.8in) Height: 368mm (14.5in)
Power Consumption	24 VAC max: 61W PoE max: 43W
Environmental	
IP Rating (Dust & Water Ingress)	IP66
Operating Temperature Range	-40°C to 60°C
Storage Temperature Range	-55°C to 85°C
Humidity	0-95% relative
Shock	IEC 60068-2-27
Vibe	IEC 60068-2-64
Vandalism	IK10 except for windows
Compliance & Certifications	
FCC Part 15 (Subpart B, class A)	
CE Marked	
RoHS	
IP66	
WEEE	
NEMA 4X	
IEC 62368	
ONVIF Profile S	
Visible Light Camera	
Sensor Type	Full HD 4K 1/1.8-type CMOS
Lens Field of View	HFOV: 61.8° - 2.15° VFOV: 36.65° - 1.2°
Focal Length	6.5mm - 202mm
Zoom	Optical Zoom: 31 Continuous E-zoom to 8x
F/#	F1.55 (Wide); F4.8 (Tele)
Sensitivity	Color: 0.25 Lux (@ (f1.6 AGC On, 30FPS) B/W: 0.10 Lux (@ (f1.6 AGC On, 30FPS)
Cyber Security	

IEEE 802.1x
TLS/HTTPS
User authentication
Access control via firewall
User credentials with policy enforcement
Digest authentication

Specifications are subject to change without notice. For the most up-to-date specs, go to www.flir.com

CORPORATE
HEADQUARTERS
FLIR Systems, Inc.
27700 SW Parkway Ave.
Wilsonville, OR 97070
PH: +1 877.773.3547

SANTA BARBARA
FLIR Systems, Inc.
6769 Hollister Ave.
Goleta, CA 93117
PH: +1 805.690.6600

www.flir.com
NASDAQ: FLIR

20-1420-SEC

FLIR | The World's Sixth Sense®

APPENDIX E. DESCRIPTION OF DMA

E.1. The Challenge of Nuisance Alarms, Reliable Detection, and Cost

Excessive NARs are a major issue for all exterior intrusion detection systems, as they can negatively impact overall security system effectiveness. Sites can experience an excessive number of nuisance alarms (e.g., alarms not caused by an intruder) per day from weather, animals, and other natural occurrences, which causes security personnel to be less effective. Sites using current commercial sensor technologies typically experience elevated NAR during harsh weather conditions. The NAR issue is one-half of the problem with traditional intrusion detection system efficiency. The other half of the problem is the need to set intrusion detection sensors to high levels of sensitivity to be able to detect stealthy intruders. However, increasing detection sensitivity increases NAR. In addition to the need to detect stealthy intruders while maintaining low NAR, the cost of security continues to escalate. This makes the issue of less expensive, reliable intrusion detection systems central to the goals of the next generation security systems of the future.

Figure E 1 is a screenshot from a radar during a brief rain shower, showing approximately 100 nuisance alarms and one real alarm. With such a high NAR, it is unrealistic for the security operator to identify the real intruder. One solution to high NAR is the DMA algorithm; the expected results are shown in Figure E 2.

Figure E 1. Nuisance alarms generated during a light rain shower

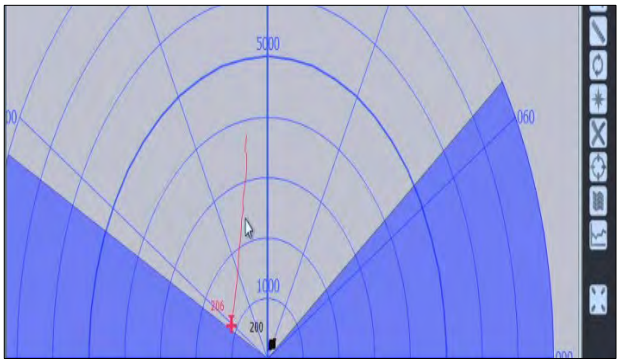


Figure E 2. Anticipated results from DMA

E.2. Proposed DMA Solution

In collaboration with Management Sciences, Inc., Sandia has developed a sensor algorithm that uses deliberate motion to differentiate alarms caused by an intruder from those caused by other natural occurrences. DMA is a multiple intelligence fusion algorithm for intrusion detection and tracking using a distributed, multi-layer tracking and classification algorithm. The DMA algorithm is capable of fusing multiple complementary sensors (such as radar, Light Detection and Ranging (LiDAR), and video) to provide reliable detection. The DMA algorithm allows elevated detection sensitivity to be set so that an alarm is declared only when deliberate motion toward a site is indicated. This technology will enable new security architectures not considered viable to date and is estimated to reduce perimeter costs by 40%.

DMA's motion pattern recognition algorithms have demonstrated the ability to identify potential intruders inside and outside the perimeter intrusion detection system, successfully issuing alarms

against positive tracks while filtering out background noise and non-threatening tracks from weather, foliage, and background traffic. When DMA determines a track to be a threat, an alarm is communicated using the standard dry contact switch, a typical alarm indication for COTS monitoring systems, making it easy to integrate with existing alarm monitoring systems. A bi-spectral pan-tilt-zoom camera, which negates the need for lighting and focuses on the DMA alarm location, provides an image of the intruder to the alarm monitoring officer day or night.

DMA's performance is based on its ability to recognize background noise and perform motion behavior analysis to focus and filter alarm indications from multiple sensors, such as filtering through the high NAR generated by video analytics scanning a grass field during windy conditions. DMA applies motion behavior analytics by aggregating the alarm position, track trajectory, and velocity of potential intruders, as reported by multiple sensor hits. DMA exploits the concept of complementary sensor phenomenology, allowing the fusion of multiple complementary sensors whose strengths augment the weaknesses of each other. Specifically, DMA combines sensor inputs in a way that allows sensors to augment physics-based limitations (e.g., an imager looking into the sun will not detect an intruder, but a radar will).

The two figures below provide real-time DMA fusion of radar and thermal radar examples at a testbed at Sandia's Sensor Test and Evaluation Center. Figure E 3 shows numerous raw radar hits (blue dots) and raw thermal radar hits (yellow dots) inside and outside a typical two-fence perimeter design. In this scenario, DMA does not declare an alarm, designated by the "No Alarm" indicator in the green circle. Figure E 4 shows DMA declaring an alarm when a track formed by both radar and thermal radar shows deliberate motion toward the secure side of the perimeter, designated by the dual-track and the "Alarm" indicator in the red circle. DMA does not just "or" or "and" the sensors, rather it decides when to "and" or "or" sensor tracks.

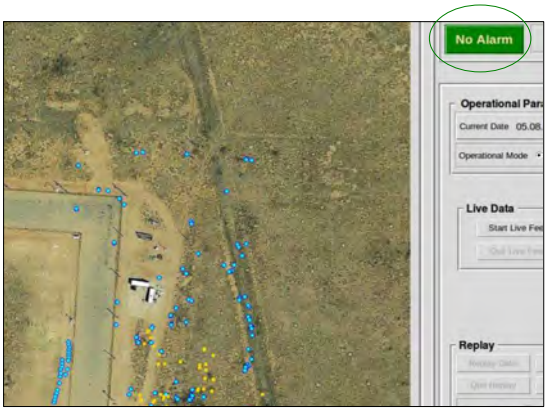


Figure E 3. DMA does not declare an alarm

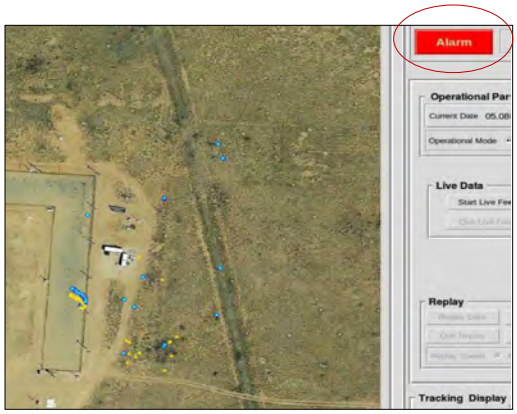


Figure E 4. DMA declares an alarm

The DMA algorithm is designed to be sensor-agnostic, meaning it should be able to fuse sensor outputs from emerging and traditional intrusion detection sensors, including radar, LiDAR, thermal radar, video, microwaves, and buried line sensors. To date, the following sensors have been fused:

- Radar and video analytics from cameras and thermal imagers
- Radar and thermal radar
- Video analytics and a buried line sensor

It is believed that DMA represents an enabling technology for security of the future and will enable new security architectures that reduce the cost of perimeter intrusion detection and provide better detection performance than traditional intrusion detection designs.