SANDIA REPORT

SAND2013-1296
Unlimited Release
Printed February 2013

Design and Evaluation of the ReKon™: An Integrated Detection and Assessment Perimeter System

Jeffrey G. Dabling, Jason J. Andersen, James O. McLaughlin

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

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2013-1296
Unlimited Release
Printed February 2013

Design and Evaluation of the ReKon™: An Integrated Detection and Assessment Perimeter System

Jeffrey G. Dabling
Intelligent Systems & Controls Department

Jason J. Andersen
Robotic and Security Systems Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-1010

James O. McLaughlin
Stonewater Control Systems, Inc.
A Subsidiary of Kontek Industries, Inc.
Kannapolis, NC 28083

Abstract

Kontek Industries (Kannapolis, NC) and their subsidiary, Stonewater Control Systems (Kannapolis, NC), have entered into a cooperative research and development agreement with Sandia to jointly develop and evaluate an integrated perimeter security system solution, one that couples access delay with detection and assessment. This novel perimeter solution was designed to be configurable for use at facilities ranging from high-security military sites to commercial power plants, to petro/chemical facilities of various kinds. A prototype section of the perimeter has been produced and installed at the Sandia Test and Evaluation Center in Albuquerque, NM. This prototype system integrated fiber optic break sensors, active infrared sensors, fence disturbance sensors, video motion detection, and ground sensors. This report documents the design, testing, and performance evaluation of the developed ReKon system. The ability of the system to properly detect pedestrian or vehicle attempts to bypass, breach, or otherwise defeat the system is characterized, as well as the Nuisance Alarm Rate.

ACKNOWLEDGMENTS

This work was performed as part of CRADA 1775.00, a Cooperative Research and Development Agreement between Sandia National Laboratories and Kontek Industries, Inc. All work performed under the CRADA was funded by Kontek. The authors would like to acknowledge the work of Mariusz Stanisz and Paul Cappello with Stonewater Control Systems for the ReKon software design and integration. The authors would also like to thank Martin Aragon, Austin Heermann, Nader Khalil, Timothy Chavez, and Erica McDowell with Sandia National Laboratories, for their help in conducting the various tests on the system.

Contents

Executive Summary **9**

Nomenclature **11**

1 Introduction **13**

1.1 Overview 13
1.2 Design and Evaluation Objectives 14

2 Design Overview **17**

2.1 Design Process 17
2.2 Design Goals 17
2.3 Barrier 18
2.4 Assessment 18
2.5 Detection 18
2.5.1 Photon Active Infrared Sensor 20
2.5.2 Intrepid MicroPoint II Sensor 23
2.5.3 REDS Sensor 27
2.5.4 VMD Sensor 29
2.5.5 LightLOC Express Optical Break Sensor 33
2.6 Software 36
2.7 Modular Software Design 37
2.8 Software System Capabilities 38
2.9 ReKon Prototype Hardware Configuration 39

3 Individual Sensor Characterization **41**

3.1 Individual Sensor Test Methods 41
3.1.1 Photon 42
3.1.2 MicroPoint 42
3.1.3 REDS 45
3.1.4 VMD 46
3.2 Individual Sensor Results 47
3.2.1 Nuisance Alarm Acquisition and Analysis 47
3.2.2 Performance Testing Results 48
3.2.3 Individual Sensor Results Summary 57

4 Integrated System Testing **59**

4.1 System Test Methods 59
4.1.1 Bridging Attempts 59
4.1.2 Tunneling Attempts 59
4.1.3 Climbing Attempts 60
4.1.4 Cutting Attempts 60
4.1.5 Maintenance Access Attempts 60

4.2 System Test Results 60
5 Sensor Fusion Demonstration 65
5.1 Logical Inference Sensor Fusion 65
5.2 Machine Learning Sensor Fusion 66
5.3 Data Capture and Data Overview 67
5.4 Sensor Fusion Analysis 69
6 Conclusion and Recommendations 81
7 References 85
Appendix A A-1

Figures

Figure 1: ReKon System Prototype Installation 14
Figure 2: Sensor Layout in Prototype System 19
Figure 3: Photon Sensor 20
Figure 4: Photon Hub 21
Figure 5: Photon Installation Configuration 22
Figure 6: MicroPoint Sensor 23
Figure 7: Typical MicroPoint Installation Configuration 23
Figure 8: MicroPoint Installation on Fence 25
Figure 9: Top Tension Wire Installation 25
Figure 10: Bottom Tension Wire Installation 26
Figure 11: (a) MicroPoint Fence Split and (b) Fence Split for Maintenance Access Portal 26
Figure 12: Fabric Deflection with 30 lbs. Force Applied Normal to Fabric 27
Figure 13: REDS Sensor Node 28
Figure 14: Detailed View of REDS Placement 29
Figure 15: Tower Integration with the Barrier 31
Figure 16: VMD Camera Tower 32
Figure 17: VMD Dome Camera Field of View 33
Figure 18: LightLOC Express Monitoring System 34
Figure 19: LightLOC Conduit Installation 35
Figure 20: LightLOC Conveyance through Maintenance Access Portal 35
Figure 21: ReKon Modular Software Architecture 38
Figure 22: FDB System Hardware Configuration 40
Figure 23: System Hardware Configuration in the NADS Control Room 40
Figure 24: Diagram of Test Paths 41
Figure 25: Photon Configuration Settings 42
Figure 26: MicroPoint Sensor Information 43

Figure 27: MicroPoint Configuration Parameters 43
Figure 28: MicroPoint Target Location (a) Threshold, (b) Clutter, and (c) Target Plots 44
Figure 29: MicroPoint (a) Incremental Threshold and (b) Detection Level Settings 45
Figure 30: VMD Rule Configuration 46
Figure 31: Histogram of Wind Speeds for *Sign on Fence* Alarm Events 50
Figure 32: All Recorded Wind Speeds during the Period June 7 – 30, 2012 51
Figure 33: All Recorded Wind Speeds during the Nuisance Monitoring Period, July 1 – Oct 8 51
Figure 34: Machine Learning Sensor Fusion Results @95% Confidence, 200 Trials 75

Tables

Table 1: Sensor Suite Implemented on ReKon Prototype 19
Table 2: REDS Sensor Node Algorithm Parameters 45
Table 3: Photon IR Test Results 48
Table 4: Photon Nuisance Sources and Alarm Rate 48
Table 5: MicroPoint Test Results 49
Table 6: MicroPoint Nuisance Sources and Alarm Rate 49
Table 7: MicroPoint Nuisance Sources with *Sign on Fence* Excluded from Data 52
Table 8: REDS Test Results 53
Table 9: REDS Footstep Nuisance Sources and Alarm Rate 54
Table 10: REDS Vehicle Nuisance Sources and Alarm Rate 54
Table 11: VMD Test Results 55
Table 12: VMD Nuisance Sources and Alarm Rate 56
Table 13: Individual Sensor NAR/UAR Summary Results 57
Table 14: System Test Results 61
Table 15: Machine Learning Event Distribution 68
Table 16: Machine Learning Event Distribution for Secondary Sensors 68
Table 17: Machine Learning Photon Test Results 70
Table 18: Logical Inference Photon Test Results 70
Table 19: Machine Learning Photon Results without Synthetic Training Data 71
Table 20: Machine Learning MicroPoint Test Results 71
Table 21: Logical Inference MicroPoint Test Results 71
Table 22: Assigned Event Classification for Machine Learning and Logical Inference Passive Testing Datasets 72
Table 23: Sensor Fusion Results for Passive Testing Phase 73
Table 24: Machine Learning Results without Synthetic Training Data for Passive Testing Phase 73
Table 25: Sensor Fusion Performance on System Level Testing 74
Table 26: Machine Learning Sensor Fusion Results @95% Confidence, 200 Trials 76

Table 27: Logical Inference Sensor Fusion Results 76
Table 28: Machine Learning Sensor Fusion Results @95% Confidence, 200 Trials, No Synthetic Training Data 78

Executive Summary

Today's increasingly complex and varied security environments emphasize the need for an agile, modular perimeter security system. Many government and military sites continue to demand high performance security technologies such as those afforded by a traditional PIDAS, but require additional standoff beyond the existing perimeter. Additionally, there are other customers whose requirements favor installation flexibility or cost over performance, but still demand better detection performance than granted by most commercially-available technology. To meet such varied needs, a perimeter security system needs to be configurable to meet the demands unique to each site, adaptable to the latest sensor technology and security requirements, and scalable to provide for installation at short temporary perimeters just as well as large multi-mile perimeters.

Kontek, Industries (Kannapolis, NC) and their subsidiary, Stonewater Control Systems, Inc. (Kannapolis, NC) have entered into a cooperative research and development agreement (CRADA) with Sandia National Laboratories to jointly develop and evaluate a new modular perimeter security solution that satisfies these requirements. The resulting design, the ReKon™ System, integrates artificial intelligence techniques with a robust physical barrier to integrate improved detection with assessment and access delay. ReKon allows integration of any type of sensor input from simple contact switch to video to rich XML data stream, and provides configurable data security options to meet the needs of a variety of sites. The software and networking architecture are modular and scalable, to allow implementation on a wide range of sites. ReKon allows high-level detection performance without requiring a full PIDAS installation through the use of multiple sensor types and innovative data fusion techniques that effectively manage the drawbacks faced by traditional sensor fusion methods.

After an initial twelve-month conceptual design phase and a formal design review, a prototype section was fabricated and installed at the Sandia Test and Evaluation Center in Albuquerque, NM. Testing was conducted over a period of five months, including two weeks of active performance testing to characterize the standard behavior of each sensor, and an additional two weeks of system testing designed to attempt surreptitious bypass of the entire suite of sensors. A perimeter security system cannot sufficiently increase detection performance through the use of additional sensors without suffering a significant increase in the nuisance alarm rate unless innovative approaches are considered. Thus, this project emphasized the evaluation of various sensor fusion techniques to reduce the nuisance alarm rate as compared to conventional methods.

The ReKon prototype system was evaluated with a suite of sensors including a MicroPoint fence disturbance sensor, Photon active infrared detector, a commercially-available high-definition video motion detection system, a prototype Sandia-developed ground sensor solution, and the LightLOC fiber-optic break sensor.

The conventional system simply performs a logical OR between all sensors. If any single sensor alarms, the system is considered to be in alarm state. The nuisance alarms are likewise combined. The logical inference system represents common simplistic data fusion techniques involving a logical AND, where the system alarms only if specific sets of sensors both register alarms within a 30 second time window. Finally, an innovative approach incorporating machine learning algorithms was also evaluated.

The conventional system achieved the high detection performance desired, with at least one of the sensors detecting each of the 173 system-level attacks attempted. However, the NAR was unacceptably high at an average of 8.86 alarms per day when looking at the entire suite of sensors. Machine learning requires rich data streams in order to achieve high accuracy, which were only provided by the MicroPoint, Photon, and video motion sensors. Therefore, only the 133 events involving MicroPoint and Photon sensors were evaluated by the machine learning algorithm, with the ground sensor and video motion sensor performing complementary sensing. To provide a clear comparison of performance differences between the two fusion methods and the conventional system, the MicroPoint/Photon subset of performance data is shown below.

Results comparison between sensor data combination methods, for Photon and MicroPoint data

	Combined NAR	Detection Performance
Conventional System	1.78	133/133
Logical Inference Fusion	0.16	95/133
Machine Learning Fusion	0.02	132/133

As expected, the logical inference method was able to significantly reduce the NAR, but at the expense of a large hit to detection performance. However, the machine learning approach was able to achieve an even greater reduction in the NAR while maintaining high levels of detection performance.

The ReKon system has been designed with capability for enhanced modularity, scalability, and provides for integrated delay, detection, and assessment. ReKon enables the incorporation of advanced fusion algorithms that enable a low-cost perimeter to still maintain high detection performance while maintaining a low NAR. Such a system may enable the use of high performance perimeter security for reduced cost in environments previously incapable of achieving such performance due to budget or installation constraints.

Nomenclature

AC&D	Alarm Communication and Display
AIR	Active Infrared
API	application programming interface
COTS	commercial off-the-shelf
DoD	Department of Defense
DOE	Department of Energy
FOV	field-of-view
ft	feet
ft^2	square feet
IP	Internet Protocol
LED	light-emitting diode
m^2	square meters
MNB	Modified Normandy Barrier
ms	milliseconds
NADS	Nuisance Alarm and Detection System
NAR	nuisance alarm rate
P_D	probability of detection
PIDAS	Perimeter Intrusion Detection and Assessment System
PM	processor module
REDS	Rapid Extended Defense System
REST	representational state transfer
SEIWG	Security Equipment Integration Working Group
SME	subject matter expert
SNL	Sandia National Laboratories (Sandia)
SOA	service oriented architecture
SOAP	simple object access protocol
STEC	Sandia Test and Evaluation Center
SWIM	Stonewater input module
SWOM	Stonewater output module
TCP	transmission control protocol

TDR	time domain reflectometry
TRL	technology readiness level
TTI	Texas Transportation Institute
UAR	unknown alarm rate
UDP	universal datagram protocol
VMD	video motion detection
XML	Extensible Markup Language

1 Introduction

1.1 Overview

In today's security environment of increasingly varied threat scenarios, many high-security military and government installations which already have fully functional perimeter intrusion detection and assessment systems (PIDAS) are currently evaluating how to increase standoff for important assets and incorporate extended detection beyond the current perimeter. Additionally, some low- and medium-security industrial installations, such as commercial power, petroleum, or chemical processing facilities which cannot afford a full PIDAS are investigating the need to incorporate increased detection capability at their existing perimeter. Some new facilities coming online may have need for a perimeter that can provide detection, threat assessment, and delay in one integrated system which does not require the intensive ground disturbance or protracted delays required by traditional PIDAS installation.

A traditional PIDAS, with the benefit of an animal control fence and engineered clear zone, serves as the benchmark against which the performance of other perimeter security systems will be compared. However, some applications as discussed above do not have the high performance requirements that would justify the expense of a full PIDAS. Other applications may have similar high-level requirements, but may require installation more immediately than possible with a full PIDAS. There exists an opportunity for a system flexible enough to meet the needs of these various customers, able to incorporate the varied sensor systems dictated by diverse facility requirements, and sufficiently configurable to provide higher performance in some installations, while allowing trade-offs to reduce cost or improve ease of installation in others. With careful selection of components and sophisticated software-based nuisance and unknown alarm detection techniques, such a modular approach to implementing perimeter security may even allow the customer to assemble a solution that approaches the high probability of detection (P_D) and low nuisance alarm rate (NAR) characteristic of a full PIDAS.

In this environment, Kontek Industries, Inc. (Kannapolis, NC) and their subsidiary, Stonewater Control Systems, Inc. (Kannapolis, NC), have entered into a cooperative research and development agreement (CRADA) with Sandia National Laboratories (SNL) to jointly develop and evaluate an integrated perimeter security solution, one that couples access delay with detection and assessment. This novel perimeter solution was designed to be sufficiently flexible for implementation at a wide range of facility types, from high security military and government installations to commercial power plants to industrial facilities of various kinds. The underlying integration technology, derived from Stonewater's Control 1st and Energy 1st platforms, will allow this perimeter detection/assessment topology to be integrated with nearly any vehicle barrier, including an existing barrier installation, and coupled with any sensor technology necessary to meet the performance requirements and security regulations of a given site.

The ReKon™[1] system was the initial outcome of this collaboration. A prototype section, shown in Figure 1, was installed at the Sandia Test and Evaluation Center (STEC) in Albuquerque, NM in February 2012. The prototype system was implemented with a robust Sandia-designed Modified Normandy Barrier (MNB), and coupled with a variety of detection and assessment solutions to demonstrate both the effectiveness of such a solution, as well as the flexibility of the system to incorporate a wide variety of inputs. In this prototype implementation, active infrared sensors, fence disturbance sensors, and a fiber-optic break sensor are coupled with a video motion detection (VMD) sensor and a Sandia-designed ground sensor. The ability of the system to properly detect pedestrian or vehicle attempts to bypass, breach, or otherwise defeat the system will be characterized, as well as the NAR.

Figure 1: ReKon System Prototype Installation

1.2 Design and Evaluation Objectives

The main objective for this project involved designing an integrated hardware and software platform for use as a perimeter security system. The goal was to develop a system capable of detecting vehicle and human traffic, with the potential to achieve PIDAS-like performance. The design was to be of a sufficiently modular and scalable nature to allow integration of various

[1] ReKon™ is a trademark of Kontek Industries, Inc.

types of hardware and software protocols. It was to be able to incorporate various commercially-available cameras, sensors, and/or lighting systems.

Additionally, the new design was to be prototyped and evaluated. The goals for the evaluation included validation and benchmark performance testing of individual sensor systems; monitoring and collection of nuisance data with all sensor systems properly configured; evaluation of multiple types of sensor fusion algorithms; and conducting a comparison of the detection and nuisance alarm performance between the sensor fusion algorithms and the standard unenhanced collection of sensors.

2 Design Overview

2.1 Design Process

The design strategy for the ReKon project has focused on developing a flexible system which is capable of meeting the demonstrated needs of various customers throughout the world. To ensure the project was properly focused on the right goals, the conceptual design phase started only after an initial brainstorming session in March 2011 with subject matter experts (SMEs) at Sandia in the fields of perimeter security, sensor design, sensor evaluation, vehicle barriers, access delay, and security system analysis.

After a nine-month design cycle, a formal design review was held at Sandia in November 2011 to ensure the ensuing prototype testing would incorporate features desired by the relevant security experts. In addition to the security areas covered in the brainstorming session, the review panel contained expertise in response force, nuclear power plant security, alarm communication and display, secure networking, wireless sensors, robotics, and international security.

Based on SME recommendations and a desire to showcase the system's ability to integrate multiple disparate sensor technologies, the prototype system would incorporate LightLOC, MicroPoint, Photon IR, REDS (a prototype ground sensor developed at Sandia), and a commercially-available VMD system.

2.2 Design Goals

The goal is to develop a highly capable system, integrated with a vehicle barrier, that can provide effective detection and assessment for use outside an existing perimeter, or to provide a detection perimeter where none exists. Not all applications need the full P_D of a PIDAS, nor can they afford the price tag. Thus, one of the primary design goals for the project is to develop a system that can be installed for less than the cost of a full PIDAS. The principal performance goals for the prototype system include: robust vehicle barrier, detection of vehicle impact, detection of personnel crossing the barrier, detection of breach attempts, detection of attempts to move or dislodge the barrier, tamper detection, and video assessment.

Additionally, the system should be modular and scalable. Each customer site will have different needs, and the system should be able to accommodate the sensors and assessment technologies that best fulfill those needs. The ReKon system was designed as an enhanced integration system. It is sufficiently flexible to allow installation on various types of vehicle barriers and integration of any available sensor, whether that sensor outputs XML, text, packed binary format protocols, analog voltage, or a dry contact closure. To achieve the modular goal, the prototype was designed to be self-contained as much as possible, such that a section of the system could be built off-site, and dropped into place with little onsite construction. To that end, a field distribution box was mounted directly to the barrier, and towers were integrated into the barrier design without need for separate foundations. The towers and FDB can be seen in Figure 1. Although the integrated towers were not utilized in the performance testing discussed in this

report, they offer the capability of mounting cameras, illumination systems, or other equipment as desired.

2.3 Barrier

The barrier chosen for the prototype was the Modified Normandy Barrier (MNB, [1]), designed by SNL. The intent of the ReKon system is to be barrier agnostic. Thus, while this barrier has been chosen for the prototype, it is not meant to indicate that only the MNB can be used with this system. The MNB was selected due to the high vehicle crash test rating [2], ability to install it with minimal digging, and current popularity with many customers due to the capability of a protective force to shoot through the barrier, making it ineffective for an adversary to hide behind the barrier. It has been crash-tested at Texas Transportation Institute (TTI), and achieved an M50/P1 rating when configured with in-ground bollard supports installed every 40 ft (12.2 m). Additionally, characterization of the barrier against both mechanical and explosive breaching has previously been conducted [1].

2.4 Assessment

This project achieved assessment through human verification via video feed, utilizing a commercial off-the-shelf (COTS) high definition day-night dome camera, purchased as part of a VMD system.

The main purpose of this project was not to verify the capability of this COTS camera for assessment purposes, but to evaluate the VMD as part of the detection package. Proper assessment for classification of a 1 ft target requires a minimum of 8 pixels (6 TV lines) of horizontal resolution, night illumination, and distribution of illumination (it is typical to aim for a 4:1 light to dark ratio), which was not verified. In a field deployment of this system, the video system would be designed to the criteria mentioned above. Additional cameras would be incorporated to ensure adequate assessment for classification of targets [3].

2.5 Detection

The prototype barrier section included various complementary sensors to better evaluate the capability of the system to integrate multiple types of inputs. Table 1 tabulates the sensors used. A diagram demonstrating how the sensors were arranged on and around the barrier is shown in Figure 2. The barrier was configured with a maintenance access pathway to mimic the needs of some installations which require breaks in outer perimeters for maintenance or patrol access. An infrared break-beam sensor, the Photon IR system, was installed across this maintenance access. An 8 ft (2.44 m) chain link fence was mounted to the front of the barrier, as can be seen in Figure 1, to enable installation of the MicroPoint according to the manufacturer's recommendations. These sensors serve to provide line detection against pedestrian attempts to climb over the vehicle barrier, or unauthorized access through the pathway. Thus, MicroPoint and Photon IR are mounted effectively in series, each protecting a different portion of perimeter (fenced versus maintenance access), and cannot be considered complementary. The vulnerability associated with line sensors is the susceptibility to bypass by bridging or tunneling the sensor.

Table 1: Sensor Suite Implemented on ReKon Prototype

Sensor	Manufacturer	Model	Hardware Version	Firmware/ Software Version
Photon Active Infrared	Deitech	PHO-2515-06EXH	PH-HUB-TC-S-01	—
MicroPoint	Southwest Microwave	Intrepid II	0x0200	64A46370-A01, Rev F
REDS Ground Sensor	SNL	—	1.1[1]	March 2011
VMD[2]	—	—	—	—
LightLOC Fiber Optic	Woven Electronics	Express	8X00051-004-RC	—

Note 1: REDS Hardware version 1.1, with mod 1 of the 'pod' enclosure system
Note 2: Specific details on the VMD system are withheld at the manufacturer's request

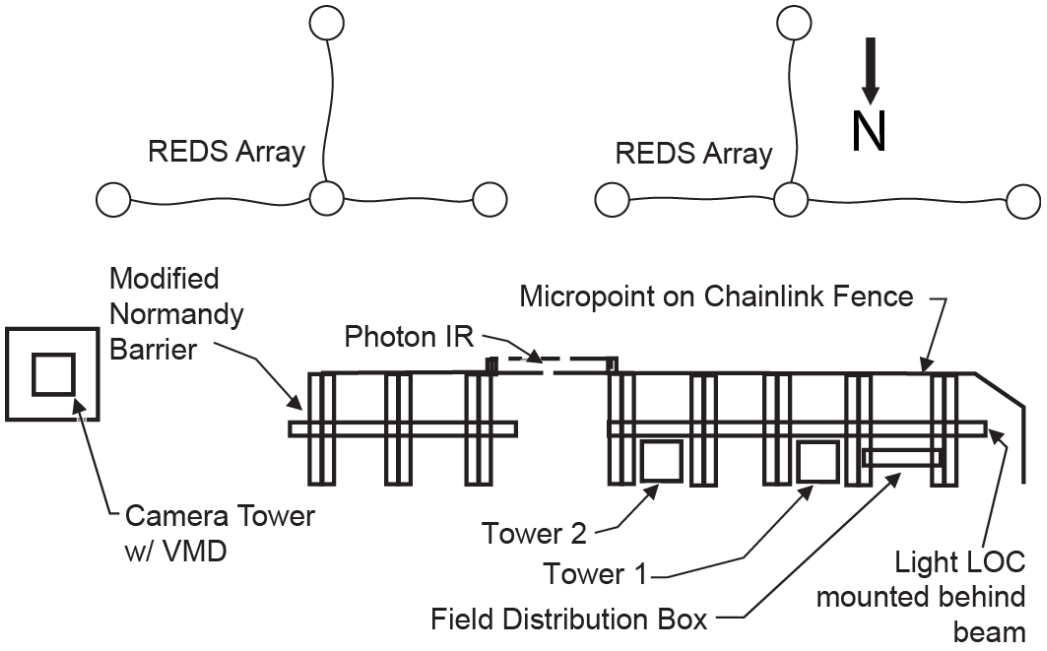


Figure 2: Sensor Layout in Prototype System

To provide complementary detection against pedestrian and vehicle threats, additional sensors were mounted off the barrier. A commercially-available day/night high definition camera with integrated VMD was mounted on a mobile camera tower east of the barrier to enable full view of the entire test section and surrounding area. A full installation may have used one of the integrated towers for the camera mount, but the short length of this test section dictated the need for a remote tower to keep the entire test site in the field of view (FOV). The Rapid Extended Defense System (REDS, [4]), a prototype seismic ground sensor system developed by SNL, was installed in the ground on the unprotected (south) side of the barrier. The LightLOC fiber optic system was used alone for detection of vehicle impact or breaching attacks, however it will provide little or no detection of personnel attempting to cross the barrier. The cable was mounted on the secure side surface (north facing surface) of the horizontal beam of the MNB, to hold it securely and couple any deformation of the barrier to the fiber.

The theory of operation, known degradation factors, and known nuisance sources for each individual sensor are detailed below.

2.5.1 Photon Active Infrared Sensor

The Photon AIR System is manufactured by Deitech and distributed by Safeguards Technology, LLC. Photon is a COTS intrusion-detection system that uses infrared technology to trigger alarms when an intruder crosses the plane of the detection field (i.e., breaks the sensor beams). It can be ordered in modules that contain from 2 to 8 beams, with heights of 27 inches (.69 m) to over 83 inches (2.1 m).

These modules, called bars, come in pairs and face each other to form a very narrow detection region the height of the upper beam, as illustrated in Figure 3. Three different configurations are available, with maximum separation distances between bars of 25 m, 50 m, and 75 m. Choosing the correct bar set with the proper separation distance during the application design is important. The two bars comprising the sensor pair must be purchased as a matched set and must stay configured together to ensure proper functionality. If one sensor bar must be replaced due to a malfunction or other problem, the entire set must be replaced.

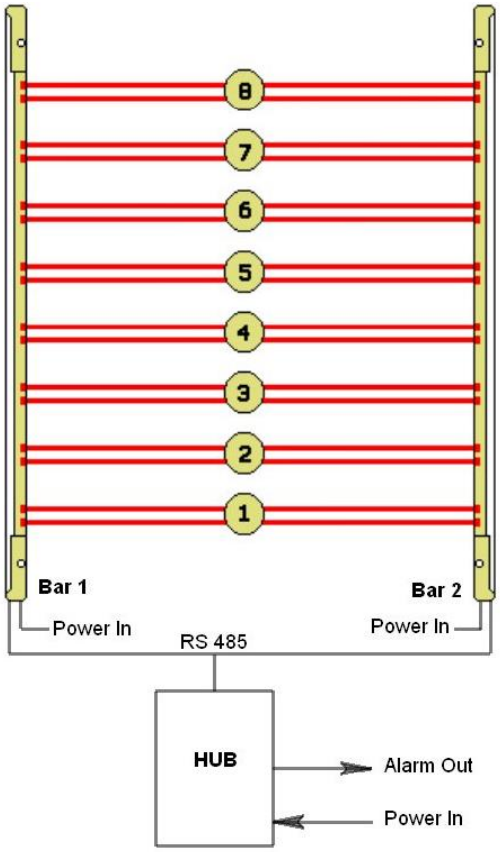


Figure 3: Photon Sensor

2.5.1.1 Sensor Function

Photon is comprised of sets of bars controlled by a hub. Each bar in a set is both a transmitter and receiver and houses an infrared light-emitting diode (LED) with a corresponding infrared detector on the opposite bar at every beam location. At every beam location (6 total for our version, with 8 possible), there are an opposing set of LEDs and detectors, which equates to one LED and one detector per beam location on the bar. The LED and detector locations are spaced

vertically, approximately two inches apart at each beam location. Deitech claims this configuration prevents a bright light source (rising or setting sun) from blinding the receiver. The bars can be setup in two different beam patterns, direct and crossed. The minimum separation distance for the sensor bars is increased for the crossed configuration. Previous work has investigated the crossed configuration and noted it worked as well as the direct beam but could potentially have a higher NAR because it covers more area than the direct beam pattern.

To create an alarm, two IR beams must be blocked; if a small object (e.g., a large insect) blocks just one of the LEDs, the event will be ignored. The bottom beam (beam 1) is specified to be 7.87 inches from the bottom of the bar housing. The same is true of the top beam relative to the top of the unit. The rest of the beams are spaced 9.8 inches apart. There is one aiming adjustment available. For horizontal beam adjustment, the entire internal assembly can be rotated ± 90 degrees. The unit should be able to operate with up to a 30 degree vertical misalignment. The hub (Figure 4) communicates to the bars via RS 485.

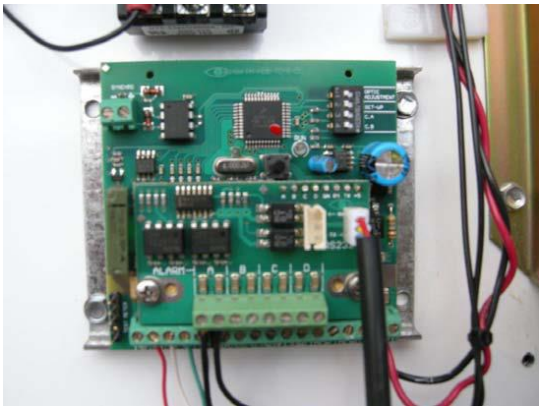


Figure 4: Photon Hub

Each hub can control up to 4 sets of bars. The hub controls the beam sequencing to prevent interference between sets of bars and it allows various adjustments to each set. These adjustments include: turning off individual beams, adjusting beam interruption time, beam sequencing time, and operating range. The hub can be fitted with an optional expansion board to provide individual relay outputs for alarms from each set of bars.

An important detection setting of note is the *beam sequencing* variable. The default is 100 milliseconds and this sequencing speed has been determined to not be sufficient to detect swiftly moving intruders, so it was determined in other evaluations that increasing the beam sequencing speed to 50 milliseconds is sufficient [5]. This results in a beam block duration setting of 0.05 seconds for both single and multiple beams. Additionally, the bars support tamper protection. A tamper alarm is triggered if the front plates of the bars are removed or the bar is removed from its mounting surface.

2.5.1.2 Known Degradation Factors

Accumulated snow cover is a potential performance degradation source, as the manufacturer indicates snow levels may interfere with beam transmission, reception, or both. Ice may divert the direction of the beam. Deitech offers sensor bar arrays that incorporate an on-board heating system, claiming this nullifies the icing issue. These issues are reported by Photon in the form of

a *disqualify* alarm that occurs if the infrared signal is severely attenuated for a length of time (i.e., due to heavy fog or the issues stated above). The disqualify function has several adjustments available on the hub, and it can be disabled if desired. During testing, when one beam was attenuated enough to cause a disqualify alarm; the sensor would still produce an intrusion alarm when any of the beams were interrupted. The fail and disqualify alarms are common collector-type outputs and will likely need to drive relays in order to be compatible to most alarm data systems. This has been fielded by SNL and worked in temperatures as low as -6° Fahrenheit. Additionally, maintenance personnel must ensure that the bottom beam remains at the desired height from the ground to ensure crawling protection since the bottom beam by default is manufactured too high to detect a low profile crawler.

2.5.1.3 Known Nuisance Alarm Sources

The nuisance sources for this sensor are adverse weather conditions such as a heavy fog. Rain tests have been conducted in 2 inches/hour conditions with no degraded intrusion detection results. Other sources include small animals that will typically trigger the lower beam locations (beams 1 and 2), but also any large birds that fly through the sensor at speeds less than roughly 27 ft/sec (18 mph). The individual beams are sequenced every 50 ms, such that one beam on the sensor system is activated every 8.33 ms (for the 6-beam model).

2.5.1.4 Sensor Placement

Figure 5 shows the installation configuration of Photon protecting the maintenance access portal. The sensor bar was mounted to angle iron and the paired bar is directly opposite the bar shown in the figure.

Figure 5: Photon Installation Configuration

2.5.2 Intrepid MicroPoint II Sensor

The Intrepid MicroPoint II sensor is manufactured by Southwest Microwave (Tempe, AZ). It is a COTS intrusion-detection system that uses fence disturbances to trigger alarms. It consists of a processor module (PM), fence cable, and link or termination units if necessary. Figure 6 and Figure 7 show the sensor cable and a PM and the typical installation configuration. It uses time domain reflectometry (TDR) technology to detect cuts and climb attempts on the fence fabric. Each PM can support up to 400 meters of cable. Up to eight PM units can be connected providing a total fence perimeter sensor of two miles in length. MicroPoint does not require additional power and communications infrastructure since it multiplexes data and communications on the sensor cable's center conductor. The software allows free format zoning between three meters and the maximum zone length.

Figure 6: MicroPoint Sensor

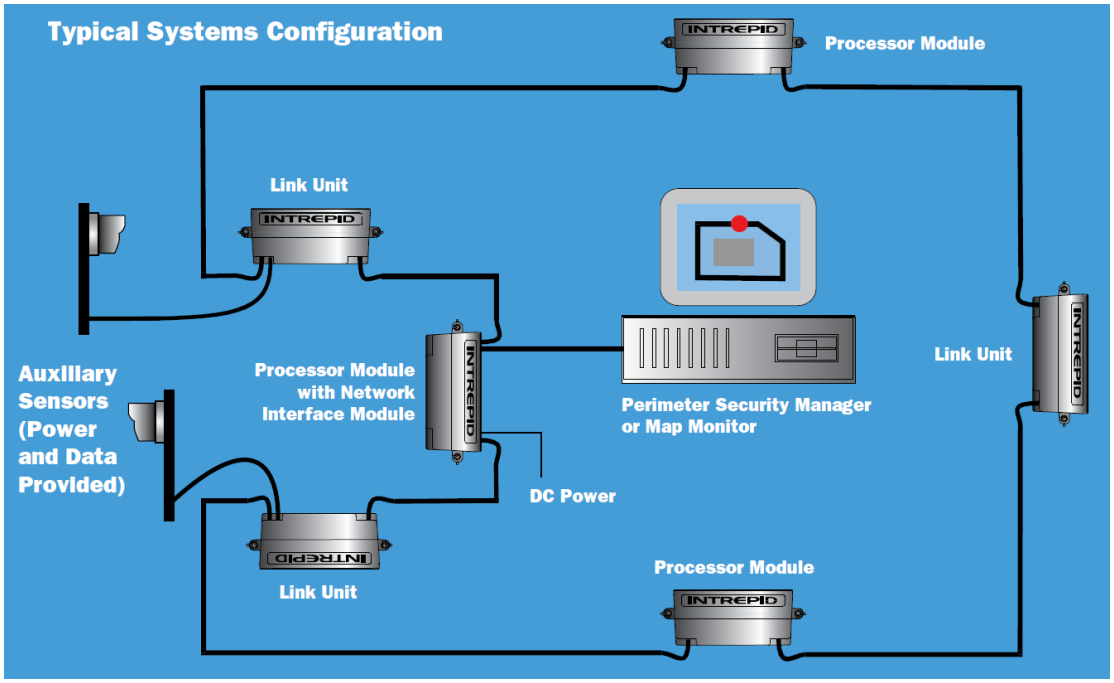


Figure 7: Typical MicroPoint Installation Configuration

2.5.2.1 Sensor Function

The PM sends pulses at a constant rate down the center conductor of the cable, creating an electric field within the cable. When the fence is disturbed, sense wires in the cable move through the electric field inducing a pulse at the point of intrusion. The pulse reflects back to the PM, which calculates the time delay to precisely locate the intrusion within three meters. Sensitivity leveling (dynamic threshold) is incorporated in the sensor cable on a meter by meter basis which automatically compensates for fence variations making each meter of fence equally sensitive to intrusions. Once a sensitivity level profile is established a calibrated threshold is set for the entire length of the cable. In addition, up to 20 control segments can be created to modify the threshold and detection window.

Each PM has two sides, A and B, and supports up to 200 meters on either side. It minimizes the NAR and unknown alarm rate (UAR) using point impact discrimination by dividing the cable into 190 subcells, each 1.1 meters long, and comparing disturbances in the source subcell and adjacent subcells. The PM provides a fail alarm in the case of power failure, cable fault, or component failure. The link unit is required between PMs when cable length exceeds 200 meters on one side of a processor module as illustrated in Figure 7. The termination unit is required when the fence sensor is used in an open loop configuration as is the case for our prototype system.

2.5.2.2 Known Degradation Factors

High winds, hail, and heavy rain conditions can degrade performance on the fence sensor.

2.5.2.3 Known Nuisance Alarm Sources

Although the sensor uses the regional subcells to minimize the NAR from global disturbances during high winds and rain, nuisance alarms are still attributed with high wind and heavy rain. Small animals that can come into contact with the fence fabric can cause nuisance alarms.

2.5.2.4 Sensor Placement

MicroPoint was installed on the fence fabric with zip ties every three chain links as shown in Figure 8. The PM was installed on the west-most fence fabric. The sensor cable was configured as one continuous zone.

Figure 8: MicroPoint Installation on Fence

Figure 9 and Figure 10 show the fence installation, with top and bottom tension wires used to provide tension in the fence fabric. The fence does not have all the recommended features of a fence that would be used for a PIDAS fence, but this was to mimic non-ideal conditions found in some installations. The goal was to find a fence sensor that could perform well on a non-ideal fence installation to promote cost savings. The fence does not have top or bottom rails installed. Additionally, the top tension wire was not secured to each fence post (Figure 9).

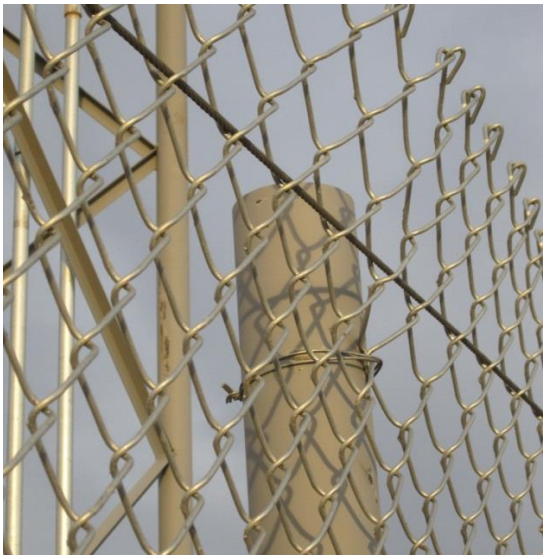


Figure 9: Top Tension Wire Installation

Figure 10: Bottom Tension Wire Installation

Figure 11(a) represents a case where a maintenance portal creates a discontinuity in the perimeter. MicroPoint was routed down the fence pole into conduit and ran underneath the cable tray and then continues to the next fence sector. Figure 11(b) shows the small fence sector after the maintenance access portal.

(a) (b)

Figure 11: (a) MicroPoint Fence Split and (b) Fence Split for Maintenance Access Portal

Figure 12 shows the fence fabric deflection (measured in inches) in the center of each panel with a 30 pound force applied normal to the fabric. There was no measureable deflection from the fence poles.

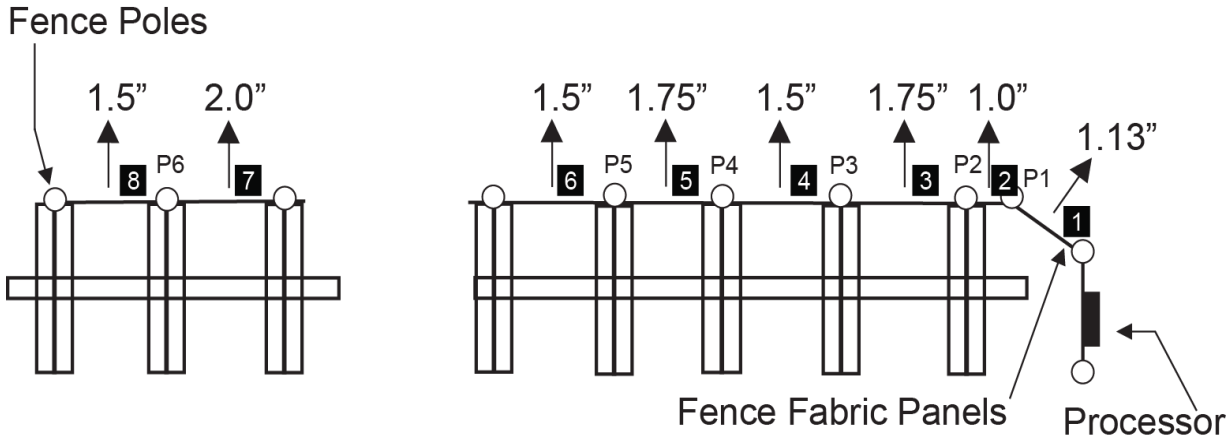


Figure 12: Fabric Deflection with 30 lbs. Force Applied Normal to Fabric

For testing purposes the fence panels and poles were labeled according to the scheme in Figure 12. The pole numbers are denoted by “PX” where “X” is the number of the pole and the panels are labeled by the black square with the number.

2.5.3 REDS Sensor

Sandia National Laboratories has developed a *beyond-the-perimeter* sensor and assessment defense system called Rapid Extended Defense System [4]. Already tested in varying field environments, the REDS system is tailored to meet specific challenges. Each REDS array consists of sensor nodes (Figure 13), which support various types and quantities of sensors. The sensor used in this prototype is a geophone sensor. The sensor data is fed into one of two different detection algorithms, footstep or vehicle. A single node can be configured to run either algorithm, but not both simultaneously. The system is still under development, with the footstep algorithm estimated at Technology Readiness Level 7 (TRL[2]), while the vehicle algorithm is more recent, and considered to be TRL 5. These separate algorithms are intended to analyze the data and ignore nuisance sources, such as animal traffic, but specifically identify whether a target is a vehicle or a human.

[2] See Department of Defense, *Technology Readiness Assessment (TRA) Guidance*, April 2011. http://www.acq.osd.mil/chieftechnologist/publications/docs/TRA2011.pdf

Figure 13: REDS Sensor Node

Sensor nodes communicate via radio frequency links with each other and send data to a Command Center, or to standalone systems in the field. Security operators can alert responders immediately, allowing evaluation of the situation before adversaries reach the perimeter.

REDS is flexible as it does not rely on any single sensor for detection. Each sensor node can support up to four seismic sensors that can be used as validation that an alarm occurred. REDS is designed with the goal of being rapidly deployed and tuned during initial system installation. Sensor nodes are powered by internal batteries and can last for extended periods when coupled with solar panels (as configured for this installation). It can be integrated with many different types of sensors. After installation, sensor node parameters can be modified remotely, allowing operators to adjust sensitivity settings or algorithm settings without field maintenance.

2.5.3.1 Known Degradation Factors

Any environmental conditions that raise the noise floor for the sensor will make it harder to discriminate signal from noise. This includes heavy rain and hail conditions. When using geophones in environments with soil that is not dense (e.g., sand) the detection range is reduced.

2.5.3.2 Known Nuisance Alarm Sources

Known nuisance sources for the seismic sensor include any type of ground/air shock waves that generate enough power in the correct frequency bands to look like a person or a vehicle, depending on the algorithm being used. Nearby low-flying helicopters have been known to cause alarms in the footstep algorithm, while low-flying jets can cause issues with the vehicle algorithm. Additionally, seismic activity outside the field of interest for detection, such as explosions, can cause nuisance alarms.

2.5.3.3 Sensor Placement

REDS was placed in order to detect adversaries before they get to the barrier, and is located on the unsecure side of the barrier with the sensor nodes 16 ft from the fence fabric. A total of four

nodes and 12 sensors were used on the prototype ReKon system. For each node, one sensor was located near the center node location, and three others arranged 16 to 22 ft away from the node, as shown in Figure 14, with two sets of nodes co-located with each other. The sensors attached to nodes 1 and 3 utilized the vehicle detection algorithm, while the sensors from nodes 2 and 4 utilized the footstep detection algorithm.

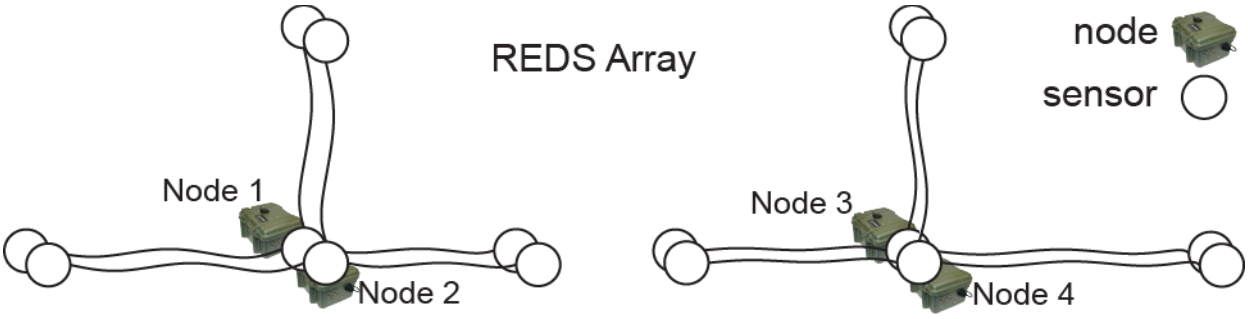


Figure 14: Detailed View of REDS Placement

2.5.4 VMD Sensor

The VMD system is a COTS intrusion-detection product that uses video to analyze an area of interest for intrusions. The system functions by classifying objects in the FOV as intrusion attempts and then triggers an alarm if that object violates the detection rules defined. It operates as an edge solution in that hardware and software required for analytics exist in the camera housing along with a local storage volume for video, whereas a centralized solution would locate all hardware and software off-camera in a remote location, such a centralized server room. The vendor provides dome cameras with onboard VMD analytics and storage solutions. Additionally, they have encoders which provide the same functionality as the dome camera package, and allow integration of 3rd party analog cameras and thermal imagers. The advantage to the dome camera package is increased resolution of the HD camera. At the time of the prototype install, the vendor could not yet take HD video from 3rd party cameras through their encoder.

2.5.4.1 Sensor Function

The VMD system has many of the same rules that you would find on many VMD analytics engines (i.e., trip wire, region of interest, fence region, loitering, etc.). The drastic difference between typical VMD systems and the one we are using is that no scene calibration is required. The operator can prepare the camera for the specific application, define a rule, and define the objects of interest, and it is ready to be used. Typical VMD systems require that you teach them about the FOV, so that they can have a spatial understanding of the object and its environment. They are implemented using shape, movement, and size to classify targets of interest and filter nuisance sources. They have an auto calibration feature which allows them to get better at classification over time.

The system provides the usual list of alarm rules which define how alarms are generated. Of greatest interest for our application are: sudden scene change detection, object moves in prohibited direction, object present in the region of interest, and object crosses a line of interest.

The typical rules define regions of interest within the FOV of the camera, target direction, target type (unidentified object, vehicle, and/or human) and a sensitivity setting.

The vendor defines the following guidelines for proper installation and optimal performance of the sensor.

- **Object Size**: In order for an object to be accurately classified, its height should be greater than 20 pixels (about 1/20th the height of the image) and less than 320 pixels (about 2/3rd the height of the image).

- **Expected Object Velocity:** The processor needs to be able to observe a moving object for approximately two seconds before classifying it. Fast moving vehicles might require a wider field of view so that the processor is able to observe them for more than a few frames.

- **Lens Selection:** Lenses should be selected and adjusted so that the objects to be detected are visible for at least four to five seconds, and are taller than five percent of the height of the field of view.

- **Blockages:** An object needs to appear unblocked for several frames in order for its classification to be accurate. When the system is used outdoors, it is acceptable for an object to be blocked during some part of the time that it is in the field of view, but a full view of the object is necessary for a good fraction of that time. When the system is configured for indoor analytics, it can detect the head and shoulders of a person.

- **Angle and Perspective:** The system expects the ground plane to be roughly horizontal, that is, people walking in the field of view are mostly upright and do not appear to be tilted due to perspective distortion. The system will function accurately if it is mounted roughly ten feet or higher from the ground and tilted no more than 60 degrees off horizontal.

- **Reflected Light:** The camera should be positioned so that light sources, including the sun, do not shine directly into the lens. Indirect light sources should also be carefully considered. While the camera uses an ultra-wide dynamic range imager, optical imperfections in the enclosure or the lens might temporarily blind it.

The system has two engines: an object classification and rules engine. Objects are classified as human, vehicle, or unknown objects and each object has a classification confidence level. The rules engine is aware of these objects and acts on set criteria to determine whether to trip an alarm. Per conversations with the manufacturer, the sensitivity of a rule directly maps to the confidence level of a classified target to be passed to the rules engine to determine if an alarm event should occur.

2.5.4.2 Known Degradation Factors

The known degradation factors for VMD systems are conditions where the analytics cannot function properly due to a degraded FOV of the camera. This is due to scene illumination during nighttime operation, heavy fog, inclement weather, and bright spots in the FOV.

2.5.4.3 Known Nuisance Sources

The specific nuisance sources other than normal nuisance sources for this sensor are not known since no previous formal evaluation has been conducted. However, known nuisance sources for VMD systems in general are adverse weather conditions (e.g., heavy rain, heavy snow, dust storms), small animals, and object shadows.

2.5.4.4 Sensor Placement

The barrier has two towers integrated with the MNB as seen in Figure 15. The goal for the integration is to optimize cost and modularity of the towers for cameras, lighting, and potentially other sensors or systems.

Figure 15: Tower Integration with the Barrier

Due to the location of the integrated towers a third tower offset from the barrier was required in order to obtain the FOV required by the VMD system for adequate coverage of the entire barrier (Figure 16).

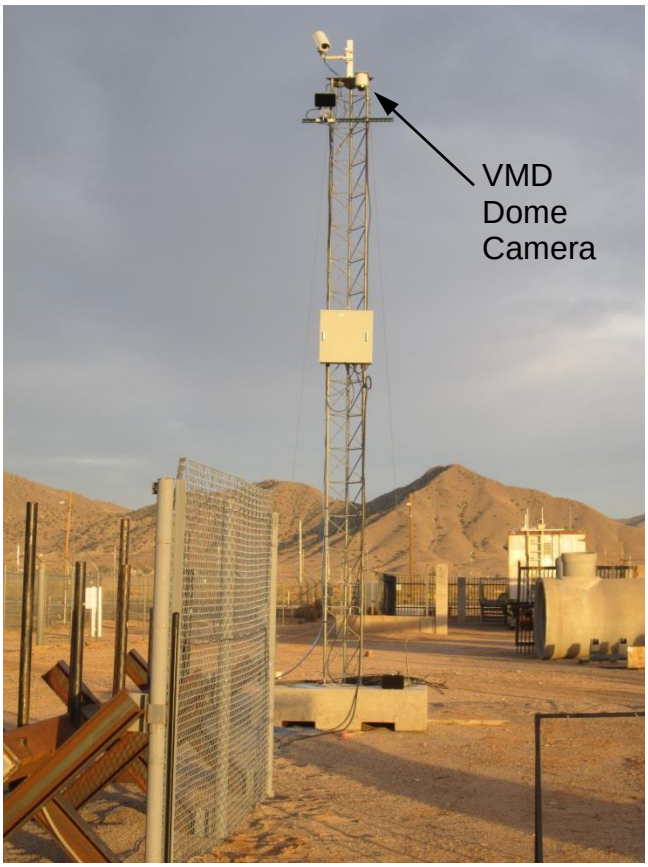


Figure 16: VMD Camera Tower

Figure 16 shows the installation of the VMD dome camera on the top of the portable tower, while Figure 17 shows the FOV of the dome camera. The camera was aimed so that the horizon was not visible in the FOV to minimize the camera blooming affects during sunset and sunrise conditions. It is noted that this phenomenon was experienced during sunset conditions. It is recommended to install a sunshade on the dome camera if it were to be deployed in a fielded system.

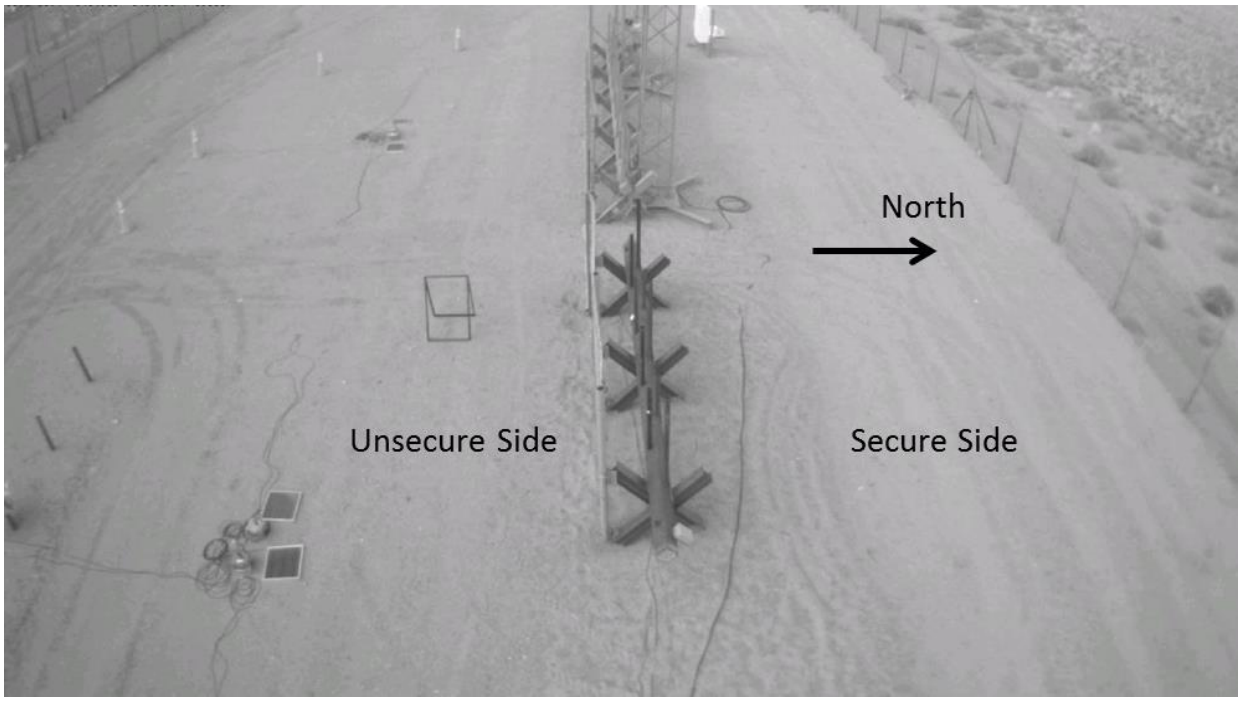


Figure 17: VMD Dome Camera Field of View

2.5.5 LightLOC Express Optical Break Sensor

LightLOC is division of Woven Electronics (Simpsonville, SC). LightLOC manufacturers a fiber optic cable that uses optical power level and thresholds to detect intrusion attempts. It is typically used in barriers and other components to detect tampering and/or damage. It consists of a light source, optical receiver, and fiber optic cable that detect degraded or no light conditions.

2.5.5.1 Sensor Function

The Express monitoring system (Figure 18) consists of the source and receiver and ports for the fiber optic cable to connect to. It can differentiate between a sensor breach and a fiber break and is rated for indoor or outdoor use. It is capable of monitoring up to 25 km. It generates a momentary breach and latched breach alarm in response to fiber tampering or a fiber break.

Figure 18: LightLOC Express Monitoring System

2.5.5.2 Known Degradation Factors

There are no known degradation factors for this sensor except for hardware and fiber optic cable fatigue.

2.5.5.3 Known Nuisance Sources

There are no known nuisance sources for this sensor due to sense modality other than equipment/component failure either transient or permanent.

2.5.5.4 Sensor Placement

LightLOC was attached directly to the main beam of the barrier. Square conduit was welded to the beam and the fiber optic cable was pulled through the conduit (Figure 19a). Figure 19b shows the routing of the other cables for connectivity of all the other systems on the barrier. LightLOC was run in conduit and under the cable tray for the maintenance access portal (Figure 20).

(a) **(b)**

Figure 19: LightLOC Conduit Installation

Figure 20: LightLOC Conveyance through Maintenance Access Portal

2.6 Software

The system software architecture reflects the physical barrier's use of modularity to adapt to diverse installation environments. Like the barrier, the software must be able to accept specialized sensor suites and fusion rules to match site conditions, and accommodate customer-specific security policies and legacy system integration requirements. A major functional requirement of the system is to provide a convenient, unified platform to integrate, monitor, and manage disparate COTS sensors. A significant problem with adding COTS sensors to a system is that each additional sensor increases the volume of nuisance alarms in the system. To address this problem, the software provides a plug-in framework to support implementing and evaluating different methods of sensor fusion to reduce the NAR. Just as there is no one-size-fits-all solution to integrated perimeter defense, the choice of algorithms to reduce the NAR will also need to be adjusted based on the sensors chosen, threat analysis, and environmental conditions. A final high-level functional requirement is to supply interfaces and adapters for integrating with existing legacy or modern command and control infrastructures. Four high-level design criteria guided the architectural decisions: *Interoperability, Extensibility, Scalability,* and *Security.*

Interoperability means supporting integration in two directions: sensor-to-system integration and system-to-system integration. Both directions require open, documented message exchange formats and application programming interface (API) contracts. Although there has been significant work to establish standardized message formats for sensors (SensorML, TransducerML, etc), few commercial sensors support these standards, and none of the sensors selected for the prototype system did. For sensor-to-system integration, a sensor adapter layer is provided to transform the raw, proprietary sensor protocol data to an intermediate XML format. This format provides a common representation for sensor fusion logic as well as facilitates further transformation into formats understood by other external systems. To provide system-to-system level integration, message formats for external APIs are implemented in XML. The APIs are exposed as representational state transfer (REST), simple object transfer protocol (SOAP), or Plain Old XML (POX) Web Services. The extensible markup language (XML) message format is based on the Department of Defense (DoD) Security Equipment Integration Working Group (SEIWG) Interface Control Document for Command and Control Display Equipment Information Interchange [6]. SEIWG is a multi-service collaboration within DoD to develop and promote interoperability standards for physical security equipment vendors, with the ultimate goal of creating an environment where true plug-and-play systems integration is possible.

To promote system extensibility and interoperability, the system was designed according to the principles of Service Oriented Architecture (SOA). The core premise of SOA maintains that all components within a system should exist as independent services with documented APIs and message formats. Applications are then constructed as compositions of these services. Services can be altered without impacting the application as long as the API remains constant, and the application can be extended or modified by reconfiguring the composition of services without touching the services themselves. The composite nature of SOA applications also improves the scalability of the system. Since each component is built as an independent service, the system supports a true distributed computing paradigm where services can be relocated to new devices as their performance requirements increase.

The ReKon system can be configured to comply with stringent site security requirements through declarative security policy files. The use of policy files allows security policy changes to be made non-invasively, without any code changes to the system software. Security policies can be applied at the transport level with Transport Layer Security 1.2[3] , or at the message level via WS-Security 1.1[4] and WS-SecureConversation[5] . Declarative policies provide the customer flexibility to decide what type of encryption and authentication the system should employ to meet facility requirements. Security policies can be executed at global enforcement points for all messages coming into or out of the system, or at local enforcement points for each system resource as it is requested. Any messages without a local or global policy authorizing it will be rejected.

2.7 Modular Software Design

The Application uses a Message Bus construct to combine services into a loosely coupled, event-driven architecture. The Message Bus creates a mediation layer that separates message producers and message consumers, providing a powerful abstraction for assembling applications out of multiple independent software modules. The Message Bus provides publish/subscribe semantics as well as lightweight orchestration of services into message-processing pipelines. Additionally, the Message Bus offers a convenient location for the consistent enforcement of security policies.

Services can be registered for any number of message channels on the Message Bus through external configuration files. The Message Bus applies security policies to incoming messages and then routes them to message channels based on rules expressed in a lightweight configuration language. Any response from a service subscribed to that channel goes back to the Message Bus to be re-instrumented just like any other incoming message. Such loosely coupled, event-driven architecture provides a powerful abstraction for creating applications out of multiple independent software modules. To add new functionality to the system, a new service is subscribed to a new or existing channel, or a new message is published to a new or existing channel. Changing the interaction between services is accomplished by altering the routing logic in the Message Bus. The Message Bus also brokers communication with external systems, such as legacy Command and Control systems, by relaying the message from the event publishing system to the destination over the correct network transport or dry contact closure relay via a Relay Translation Service. Figure 21 provides a component level overview of the ReKon System software architecture.

---

[3] https://datatracker.ietf.org/wg/tls/charter/

[4] http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[5] http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.pdf

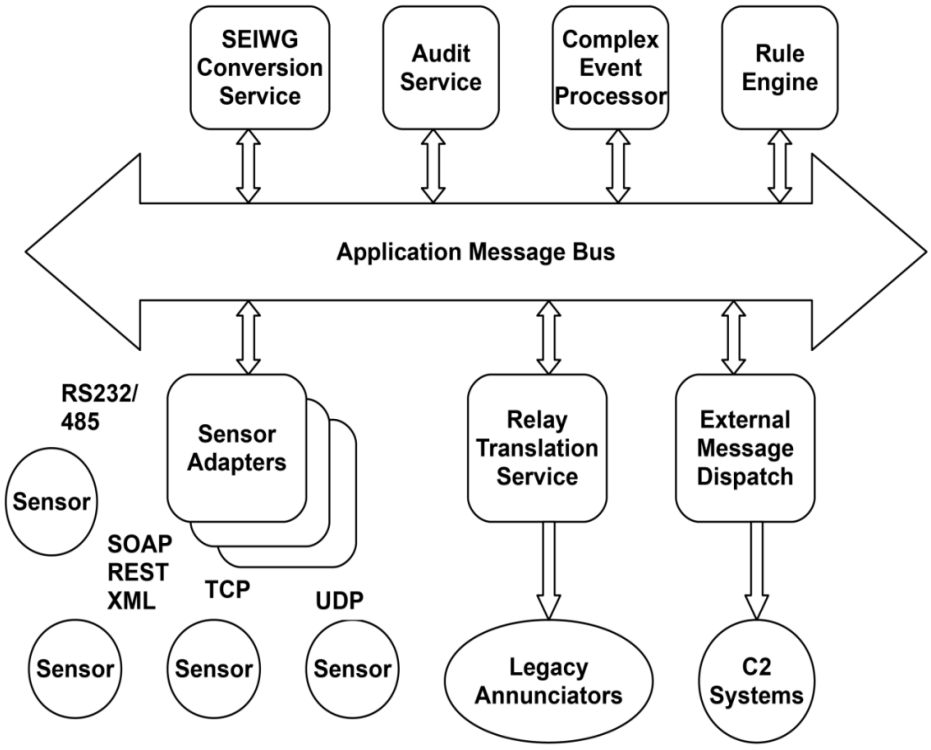


Figure 21: ReKon Modular Software Architecture

2.8 Software System Capabilities

Sensor adapters harvest real-time sensor input over a variety of communication media: RS-232/485, user datagram protocol (UDP), transmission control protocol (TCP), and hypertext transfer protocol (HTTP). Each adapter converts the raw input into an intermediate XML format and sends it to the application Message Bus. The Message Bus publishes the message to authorized internal and external consumers (services). Internal consumers include a Logging Service which records every message for auditing and analysis; a SEIWG Conversion Service which understands how to transform all internal messages into their corresponding SEIWG representation; a Complex Event Processor for fusing message streams from the different sensors; a Rule Engine which executes actions based on rules concerning changes in system (including sensor) state; and a Relay Translation Service which converts XML alarm messages into relay outputs for communication to legacy annunciators. The system also contains a service for external consumers to manage their subscriptions to message topics. Messages can be dispatched to external services through a number of transports: SOAP, REST, HTTP/S, java message service, TCP, and UDP. Custom security policies can be applied for each external endpoint.

The Complex Event Processor subscribes to all message streams in the system and executes filters against those streams to select time windows over which the streams can be combined with various logic operators, producing aggregate, or complex, events which are fed back into the Message Bus. The Rule Engine maintains a continuously updating picture of the system's state and can trigger actions based on changes to the system, such as issuing an alarm report.

The facts the Rule Engine maintains about the system, the rules it evaluates against those facts, and the resulting actions are all configurable by the user through a simplified scripting interface. The Message Bus facilitates lightweight orchestration of services with an XML-based configuration language, allowing the construction of sophisticated processing pipelines while keeping the individual services separate and self-contained.

A typical example is the REDS message workflow. Detection or status data is received by the sensor adapter, converted into XML format, and passed to the Message Bus. The Message Bus publishes the message to the appropriate topic, it is received by the Logging Service (the SEIWG Conversion Service) and the Complex Event Processor, and any responses are republished by the Message Bus. The Complex Event Processor fuses the REDS message with matching VMD and/or Photon IR messages. The Rule Engine picks up the response from the Complex Event Processor, updates its system state, evaluates any rules affected by the change, and sends the result of any triggered actions back to the Message Bus. Responses from the Rule Engine are picked up by the SEIWG Conversion Service and then published to external subscribers, or sent to the Relay Translation Service if the system is tied to a legacy annunciator.

2.9 ReKon Prototype Hardware Configuration

Block diagrams for the hardware configuration on the barrier and in the control room are shown in Figure 22 and Figure 23. It is noted that in Figure 22, the VMD, REDS, MicroPoint, and Photon sensors report more data than only alarm state. The Stonewater input modules (SWIMs) ingest alarm contacts and communicate with the Stonewater output modules (SWOMs) to change alarm state of the individual sensors. MicroPoint and Photon did not have an IP interface so a third party serial-to-IP device was used to access the data. The ReKon Fusion Engine interprets data from REDS and then drives two separate relays to signal an alarm event (one for REDS vehicle and footstep detection). The third relay driven by the fusion engine is the logical fusion relay. This relay represents the logical inference rule that was created in the system. There is no machine learning relay since the analysis of this rule did not get implemented in real time. All analysis of this rule was implemented off-line with data gathered during testing and nuisance monitoring described in Section 3.2.1. Alarm signals were monitored via an alarm communication and display (AC&D) system developed by Sandia for use at STEC, the Nuisance Alarm and Detection System (NADS). The barrier was connected to the NADS control room hardware via fiber optic cable over the network.

Figure 23 (NADS control room) represents the hardware that would be located in the equipment room in a real installation. The NADS computer monitored all alarm events from all the individual sensors. Additionally, weather data was gathered from the weather station once per minute. The NTP server synchronized time on all equipment. The sensor data recording laptop collected data for off-line analysis of machine learning algorithms used for sensor fusion.

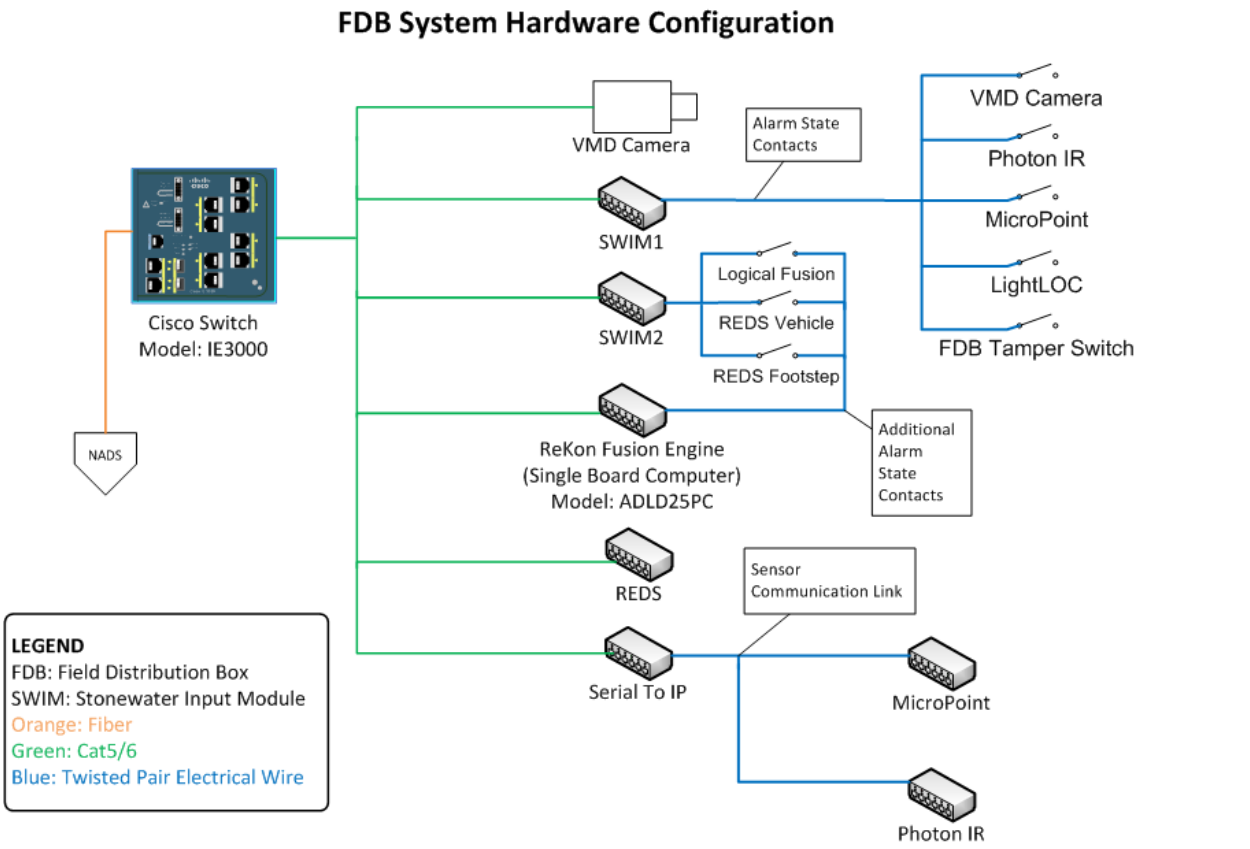


Figure 22: FDB System Hardware Configuration

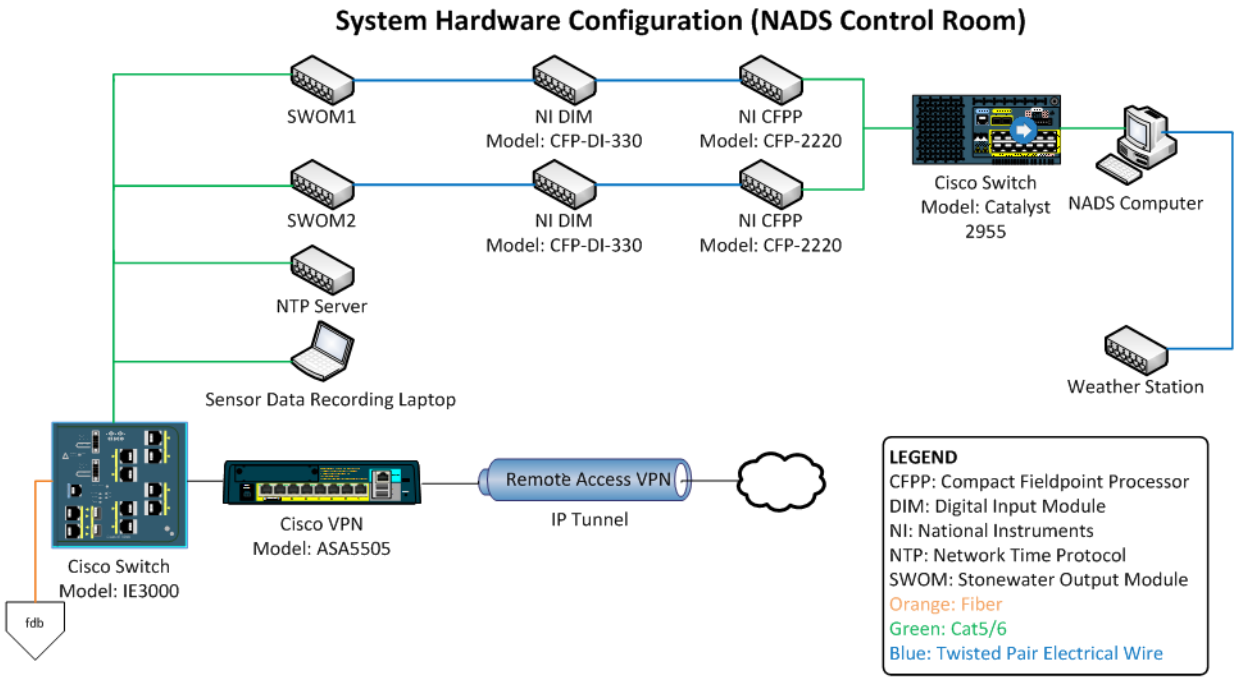


Figure 23: System Hardware Configuration in the NADS Control Room

3 Individual Sensor Characterization

Performance testing was split into two categories: individual sensor characterization and system level performance. Individual sensor testing was necessary to characterize each sensor's strengths and weaknesses, which were used to define the system-level performance testing to follow. The threat was defined to be a walking, running, belly-crawling, or bear-crawling adversary with access to a vehicle. Single adversaries and groups of three were utilized. During performance testing, test path distances and intruder speeds were recorded along with timing information.

3.1 Individual Sensor Test Methods

Characterization tests were run on each sensor, except LightLOC. It was tested only by bending the fiber or simulating a break in the fiber. During the characterization testing, various approach paths were used by the subjects to evaluate the sensors' response, as shown in Figure 24. Each test path is numbered and referenced in the sections below.

Vehicle tests were conducted using two different methods. Unless otherwise specified, the tests were run using the "Start/Stop" method, which refers to stopping the vehicle just before reaching the barrier fence. Continuous Movement, as referenced in the table III and IV by "Cont.", refers to driving through the maintenance access. For all vehicle testing, *Polaris* refers to a Polaris Ranger 2-seat ATV 4x4, while *Minivan* refers to a Dodge Caravan.

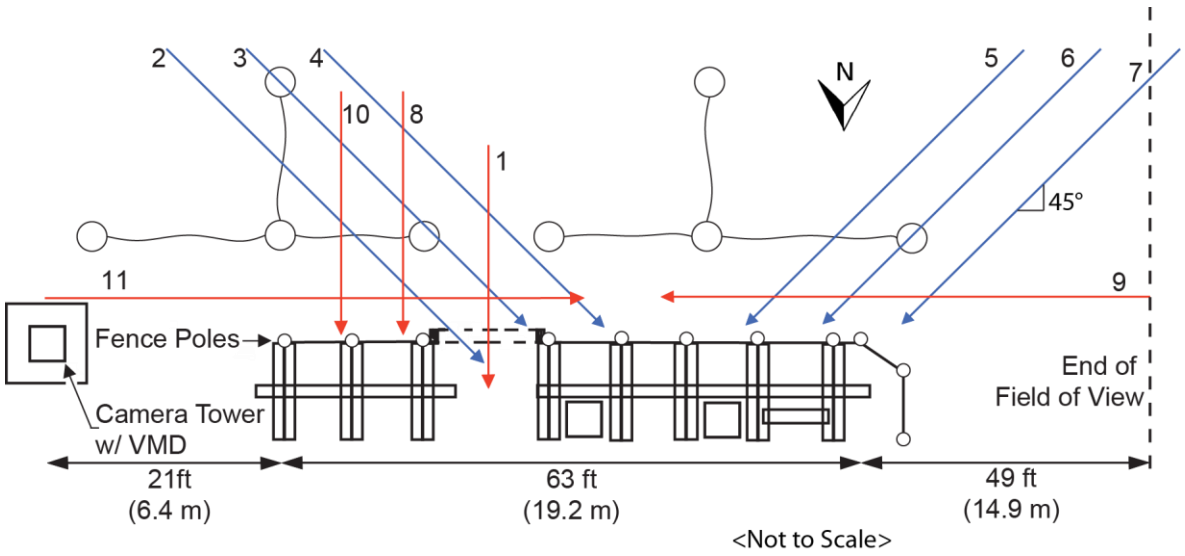


Figure 24: Diagram of Test Paths

3.1.1 Photon

The Photon IR sensor was tuned to ensure an adversary could not crawl under the bottom beam, or run through faster than the phasing of the beams. Testing included walking, running, and crawling subjects attempting to pass through the Photon IR sensor array undetected. The configuration of Photon is shown in Figure 25.

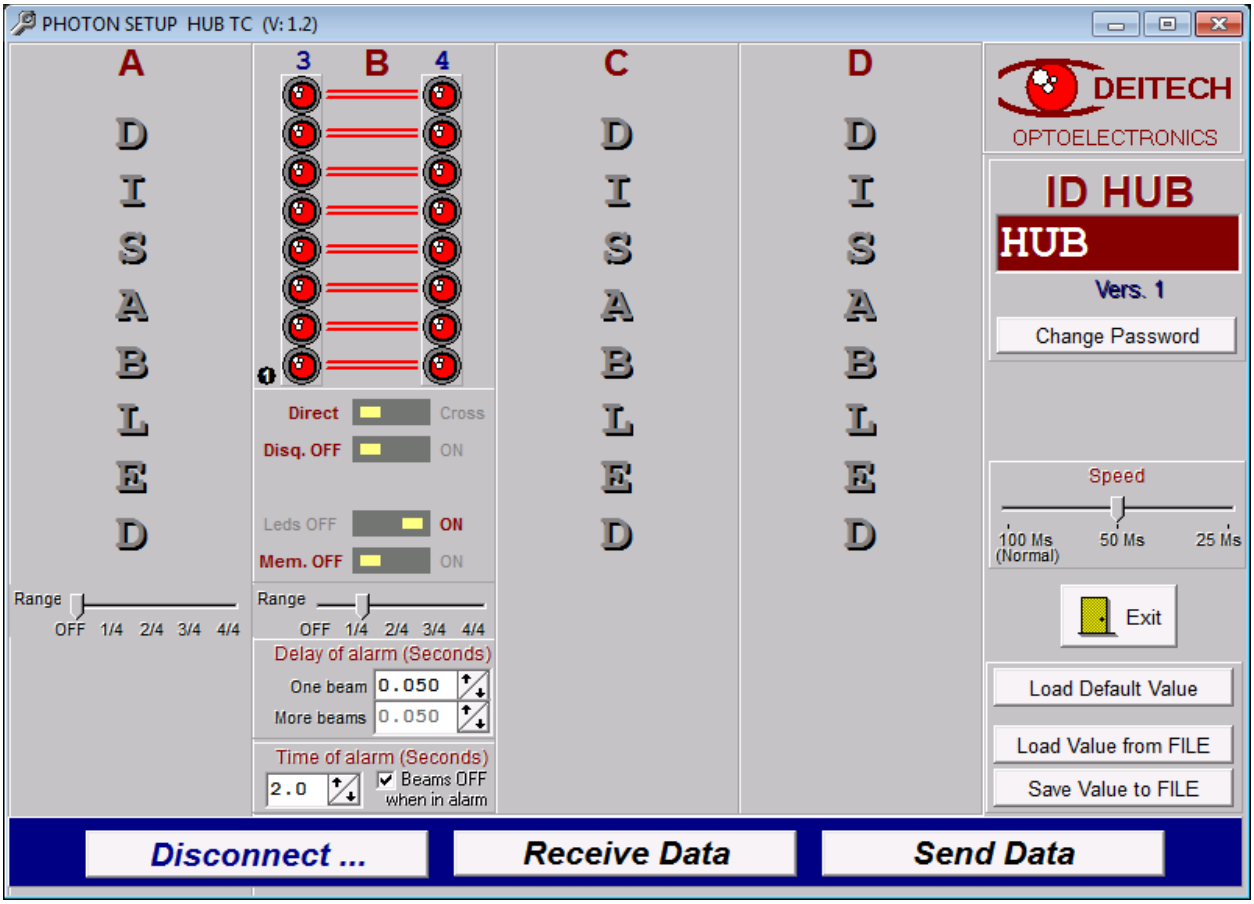


Figure 25: Photon Configuration Settings

Sandia has previous history with Photon and the settings were set according to previously conducted testing.

3.1.2 MicroPoint

MicroPoint testing consisted of subjects climbing the fence and simulated cuts. There were a total of six poles tested when climbing (referenced as P1-P6 in Figure 12), where the subject would climb on the fence at the pole location. When conducting fabric climb tests, the test subjects climbed on the fabric between poles 1–6 and an additional fabric panel adjacent to pole 1. For all climbing tests, the subject would climb to the top of the fence and hold position at the top for approximately two to three seconds. The cut tests consisted of performing no more than eight simulated cuts, 1–2 seconds between cuts, in a pattern which would form an opening at the bottom of the fence fabric. It is considered necessary to make at least 8 cuts to the fence to create an opening sufficiently large to crawl through, and thus the fence is configured to not

alarm unless a minimum threshold of events is detected. Due to the installation of a tension wire through the bottom of the fabric, no significant movement of the fabric was possible, and thus attempts to bypass the fence by lifting the fabric off the ground were not explored. The MicroPoint sensor information is shown below in Figure 26.

Sensor Information	
Sensor Address	0
Sensor ID Tag	Smart Barrier Proto
Response Timer Value [ms]	1
Alarm Poll Function Type	0x0100
Electronic Serial Number	AA:01:00:22:2D:53
Hardware Version	0x0200
Software Version	64A46370-A01 REV F
Software Build Date	2011-07-25
Software Build Time	14:47:18
Current Sensor Date	2012-11-15
Current Sensor Time	17:48:31

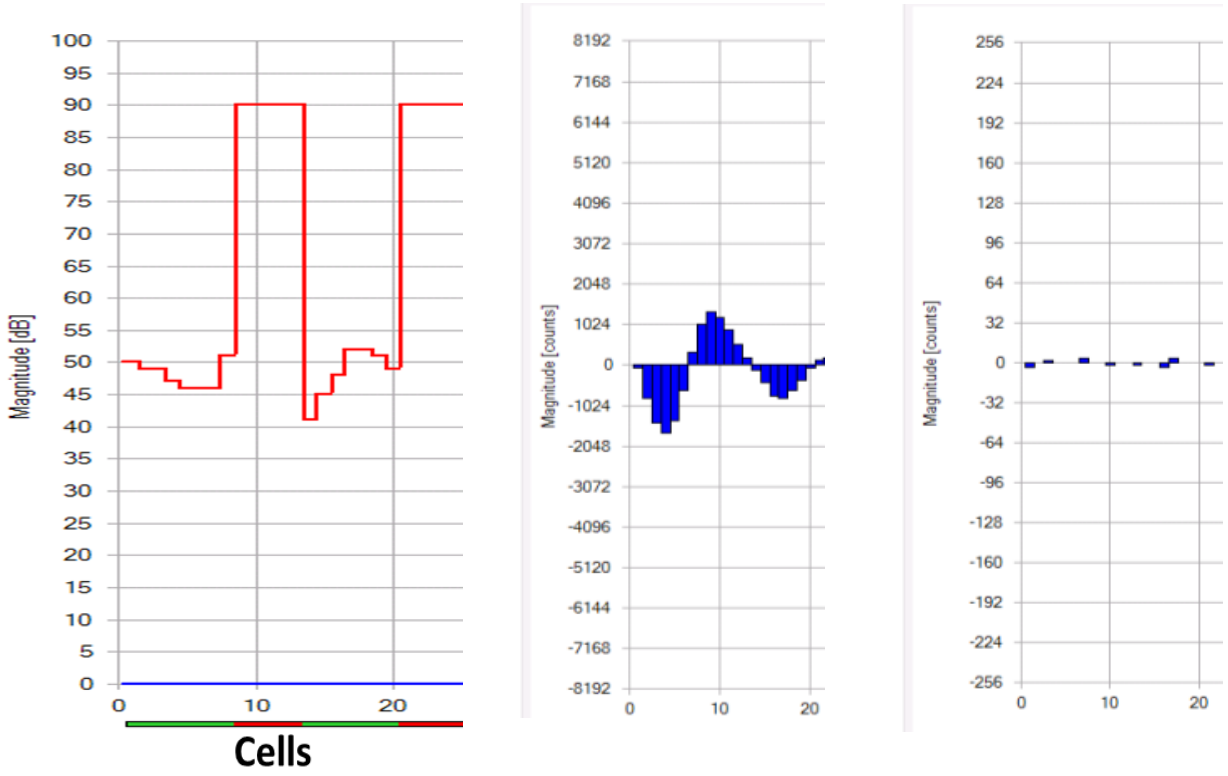
Figure 26: MicroPoint Sensor Information

Figure 27 shows Cable A configuration parameters that were all set to default.

Cable A - Configuration Parameters			
Analog Channel Gain Setting	0		Edit
Integrator Sample Length	2	counts	Edit
Threshold Factor	-12	dB	Edit
Alarm Mask Time	15	sec	Edit
Alarm Mask Window	5	cells	Edit
Alarm Hold Time	5	sec	Edit

Figure 27: MicroPoint Configuration Parameters

The calibration was performed per the Southwest Microwave manual for MicroPoint and yielded the default threshold with respect to the cell plot seen in Figure 28a.



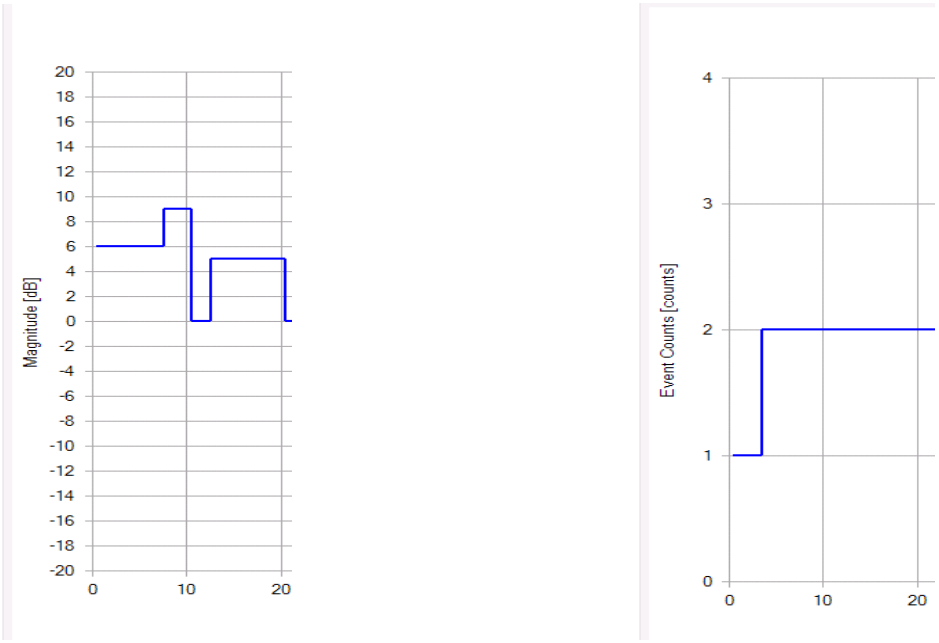
(a) (b) (c)

Figure 28: MicroPoint Target Location (a) Threshold, (b) Clutter, and (c) Target Plots

The green and red marking below the x-axis of Figure 28a denotes active and disabled cells respectively. The x-axis for each of the MicroPoint configuration plots represents distance with respect to cells. The cable is disabled from cell 9 to 13 to account for the maintenance access portal. The cable ends at cell 20. After the initial calibration was complete, preliminary testing was conducted to determine further tuning of the thresholds and count parameters to reach the desired performance. Once calibrated, the installation was validated according to the clutter and target plots in the MicroPoint II Installation Tool (Figure 28b and Figure 28c).

According to Southwest Microwave, the clutter should be between ±7168 counts and target should be between ±256 counts. That was achieved in our installation. This was checked throughout monitoring this sensor to ensure proper operation.

Figure 29a shows the adjustments to the threshold that were made after the initial calibration and Figure 29b shows the detection level settings.



(a) (b)

Figure 29: MicroPoint (a) Incremental Threshold and (b) Detection Level Settings

In response to poor performance on the corner poles and fabric in cells 1 through 3 (Figure 29b), the event count was lowered to one. Typically it is recommended to leave this setting at a minimum of two counts, however adjusting the threshold proved unhelpful in our case, so lowering the event count was necessary.

3.1.3 REDS

A detection on REDS was defined to include triggering by either the footstep or vehicle detection algorithms during the test attempts. In evaluating the data, it should be noted that REDS is a prototype system, and is not yet a commercially-fieldable system. REDS data was monitored during the running, crawling, and vehicle tests already being performed for VMD, discussed below. The footstep algorithm parameters were set according to Table 2. The vehicle algorithm does not currently have any parameters to adjust.

Table 2: REDS Sensor Node Algorithm Parameters

Parameter	Value
AspPreampGain	64
AlgNumPersist	20
AlgMinNumToDet	7
AlgKurtosisThresh	5.0
AlgNumSampPerWindow	128

3.1.4 VMD

Testing for the VMD system was conducted both in color and monochrome mode, always in the daytime. No testing was performed at night due to illuminator malfunction and project schedule. This specific VMD system did not require any initial calibration or algorithm training other than setting up user-defined rules, which were configured to alarm whenever any object classified as a person or vehicle was detected within a 6 ft (1.8 m) zone defined immediately south of the chain link fence. As subject-to-background contrast can have a significant effect on VMD performance, the effect of contrast was evaluated by varying the color of clothing worn by the subjects in comparison to the tan colored sandy soil in the test field. Thus, testing was performed at three clothing contrast levels, defined as H = high (bright white), M = medium (dark green), and L = low (light tan).

The VMD dome camera was configured to be monochrome during the day and night based on preliminary testing results that indicated the algorithm triggered an alarm earlier than when in color mode for the same attack method. The analytics engine was configured with noise filtering on and auto calibration on. Three different rules were applied to the FOV which included change of scene, directional line of interest (LOI) (red line), and object present in region (green box) as seen in Figure 30.

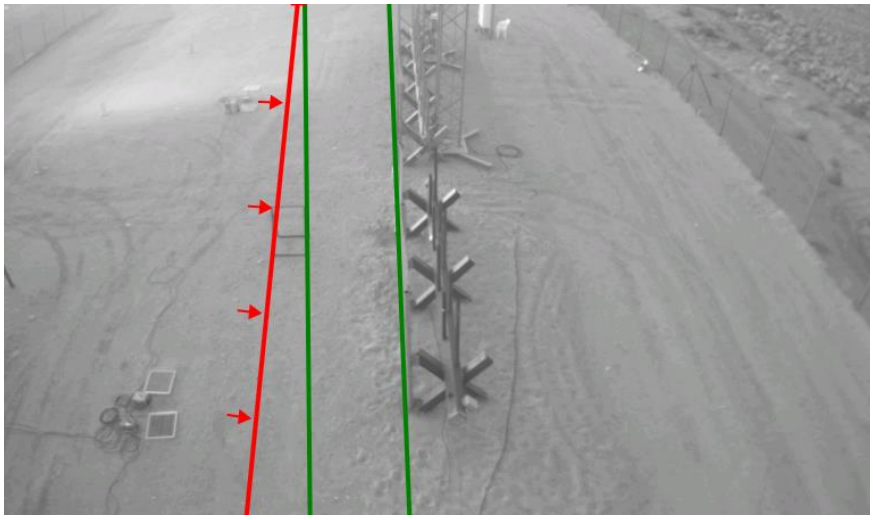


Figure 30: VMD Rule Configuration

Based on preliminary testing, it was determined that the sensitivity for the region of interest (ROI) should be set to 9 on a 1-to-10 scale (10 being most sensitive). To attempt to reduce nuisance alarms, it was not set to 10. The system had difficulty classifying several adversary approaches and commonly would not achieve classification until the adversary was against the barrier. For that reason, the ROI was set to *object present in region* and the time the object had to be in the region was set to longer than one second. The LOI rule had a sensitivity of 9 as well, and both ROI and LOI were set to trigger on only person or vehicle object types based on preliminary testing that indicated unknown object was not tripped on the conducted test sets. The scene change alarm was set with a sensitivity of 2, as higher sensitivities yielded nuisance alarms with passing cloud cover.

3.2 Individual Sensor Results

The effectiveness of a sensor against a specific attack method in a given environment is most commonly measured with the P_D, calculated with a confidence interval over the binomial distribution [7]. Additionally, the NAR is included in the results below.

3.2.1 Nuisance Alarm Acquisition and Analysis

Nuisance alarms were collected from all the individual sensors continuously from June 30 at 11:59 PM through October 8 at 11:59 PM, 2012 for a total of 98.8 days (accounting for testing periods and maintenance). NADS was used to collect alarm data for the sensors on the barrier along with weather data. An electronic record of all alarm and weather data during the period defined above is available for review (STS02120). For details of the NADS system configuration, see Figure 23. While conducting tests and collecting nuisance alarm data during this period the sensor parameters were not altered. Further, the alarms that were generated during testing and maintenance of the system and the time period associated with these events were not incorporated into the nuisance alarm rate calculations. All alarm rates are specified in units of alarms per 24 hours unless noted otherwise.

For the purposes of this work, a real alarm is when the video assessment can verify that either a human or vehicle caused the alarm. A nuisance alarm is identified as alarm related to a non-intrusion attempt (e.g. tumbleweed, rabbit, inclement weather, etc.). An unknown alarm is one for which the cause is unidentified. A fourth category of alarm was identified as Insufficient Data. This means that the ability to assess the alarm was not possible for technical reasons (e.g., camera malfunction, poor camera visibility, etc.). An insufficient data alarm could be a nuisance or an unknown alarm, but due to uncertainty this report considers those alarms as nuisances with no further classification. All insufficient data alarms occurred during nighttime hours, with the exception of the alarms due to the camera being blinded at sunset (due to camera blooming), and were considered nuisance alarms for the purposes of this prototype evaluation, as the likelihood of human or vehicle traffic through the test site at those times is very small.

The nuisance alarms for each sensor were categorized under daytime and nighttime occurrence. Daytime was defined as the time between sunrise to sunset and nighttime is the remaining time on that day. Sunrise and sunset times were referenced from U.S. Naval Observatory data [8]. The cumulative test period consisted of approximately 1288 hours classified as *Daytime*, and 1082 hours classified as *Nighttime*. Additionally, some nuisance alarms cause more than one alarm event within a defined time period (e.g., rabbit that continues to go in and out of the bottom beam of an AIR sensor). Thus, if the same nuisance source continued to create alarms within 30 seconds of the last event created, the multiple redundant alarms were collapsed to a single alarm count in the final nuisance alarm and unknown alarm rate calculations. However, Appendix A.2 includes the raw sensor alarm data for all sensors along with the corresponding nuisance alarm and unknown alarm rates and further explanation of the filter rule that was used.

3.2.2 Performance Testing Results

3.2.2.1 Photon Results

The Photon sensor functioned as expected, based on previous Sandia testing experience. Table 3 contains the test results from the varied adversary approaches. The P_D for the bear crawl is lower than the other approaches, but this is due to the number of trials run.

Table 3: Photon IR Test Results

Approach	Path	Speed (ft/s)	Detections/ Repetitions	P_D @ 95% Confidence
Walk	1	4	30 / 30	91
Belly Crawl	1	1	40 / 40	93
Bear Crawl	1	1	20 / 20	86
Run	9	14	30 / 30	91

Table 4 contains the nuisance sources and alarm rate recorded for the Photon sensor. The Photon sensor is known for a low NAR in controlled PIDAS-like environments. Sunrise and sunset are usually not an issue for this sensor; however, four alarms were generated during these events. This happened on three different days, each at different times. The Photon has transceivers on both bars, so it can detect when it is being saturated by the sun. However, upon further investigation for these events, photon data showed that bar 4 (bar facing sunset) was blinded and then beam 1 on the opposite bar tripped on each of the four occurrences. A rabbit or other small animal is also a known nuisance source for this sensor. One alarm event occurred in conditions with insufficient light to assess the cause. Only one instance of the rabbit alarm event was filtered, but in general, the Photon will trip multiple times for an alarm source that is continually breaking the IR beams.

Table 4: Photon Nuisance Sources and Alarm Rate

Alarm Source	Alarms	NAR	UAR
Daytime			
Rabbit	5	0.05	----
sub total	5	0.05	0
Nighttime			
Rabbit	1	0.01	----
Sunset	4	0.04	----
Poor Camera Visibility	1	0.01	----
sub total	6	0.06	0
Total	11	0.11	0

3.2.2.2 MicroPoint Results

The MicroPoint sensor functioned as expected, based on previous Sandia testing experience. Table 5 contains the climbing and cutting test results from the varied adversary approaches. The 30 climb tests on the fence poles were distributed by five tests per pole.

Table 5: MicroPoint Test Results

Approach	Location	Detections/ Repetitions	P_D @ 95% Confidence
Climb	On Poles	30 / 30	91
Climb	Between Poles	29 / 30	86
Cut	Between Poles	30 / 30	91

The 30 climb tests between the poles on the fence fabric were distributed by four tests per fence panel with the exception of three tests on panel 1 and 2. The one miss occurred on panel 8. Each of the three or four tests on the fence panel were distributed throughout the length of the panel. The cut tests were distributed in the same fashion as the climbs on the fence panel, with the exception that the cuts were all repeated in the same location and at the bottom of the fabric as the previous test for each panel.

Table 6 contains the nuisance sources and alarm rate recorded for MicroPoint. The only nuisances observed were weather related; otherwise the alarms were not assessable. During the nuisance monitoring period a sign was installed on the fence. It was not completely secured to the fence and was able to move in the wind. The data indicates that most of the high-wind alarms were due to the sign on the fence.

Table 6: MicroPoint Nuisance Sources and Alarm Rate

Alarm Source	Alarms	NAR	UAR
Daytime			
Sign on Fence	64	0.65	----
Poor Camera Visibility[1]	2	0.02	----
High Winds	11	0.11	----
Unknown	48	----	0.49
sub total	125	0.78	0.49
Nighttime			
Sign on Fence	319	3.23	----
Poor Camera Visibility	55	0.56	----
Rain	30	0.30	----
Unknown	19	----	0.19
sub total	423	4.09	0.19
Total	548	4.87	0.68

Note 1: Refers to camera blooming during sunset condition

The sign on the fence had no visible movement for the alarms labeled as *high winds* in Table 6. The unknown alarms had no assessable cause. In order to determine whether the alarms ascribed

to *sign on the fence* were truly due to the sign, a histogram of the wind speed for those alarm events was created (Figure 31).

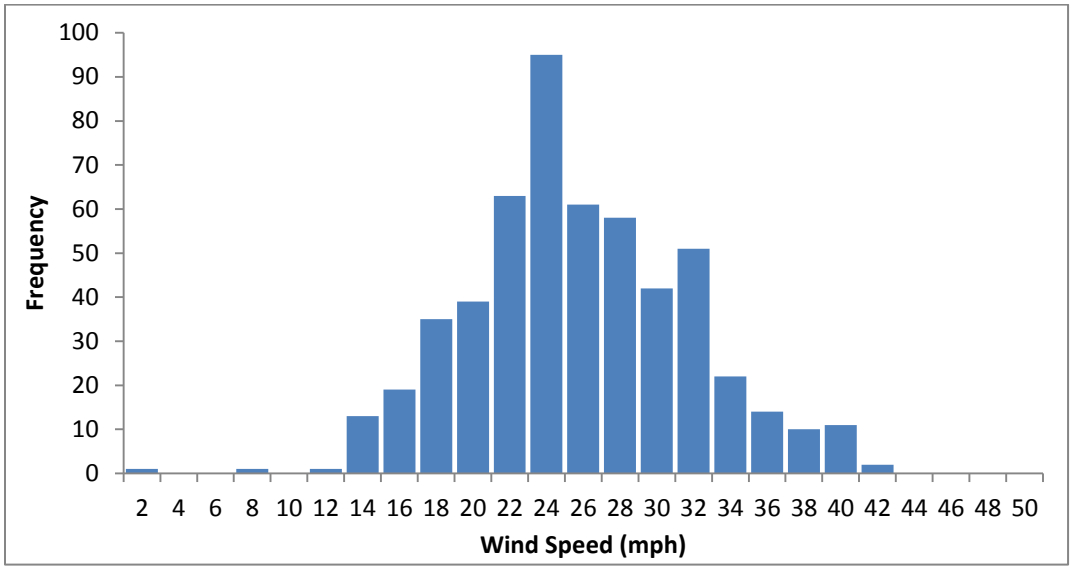


Figure 31: Histogram of Wind Speeds for *Sign on Fence* Alarm Events

The peak occurrence of winds during this period was between 22 to 24 mph. The sign was installed on 8/6/2012 and remained on the fence until 10/05/2012. This covered nearly the entire period of nuisance monitoring. However, MicroPoint was tested and calibrated by 6/6/2012. The period between 6/7 - 6/30/2012 was examined to investigate the wind speed and alarm events associated with MicroPoint. During this period there was only one unknown alarm on 6/21/2012 with recorded wind speed of 29 mph. The histogram of the wind speeds that occurred during this period is shown in Figure 32, with wind speed data points taken every minute. The histogram for all wind speeds during the nuisance monitoring period is shown in Figure 33.

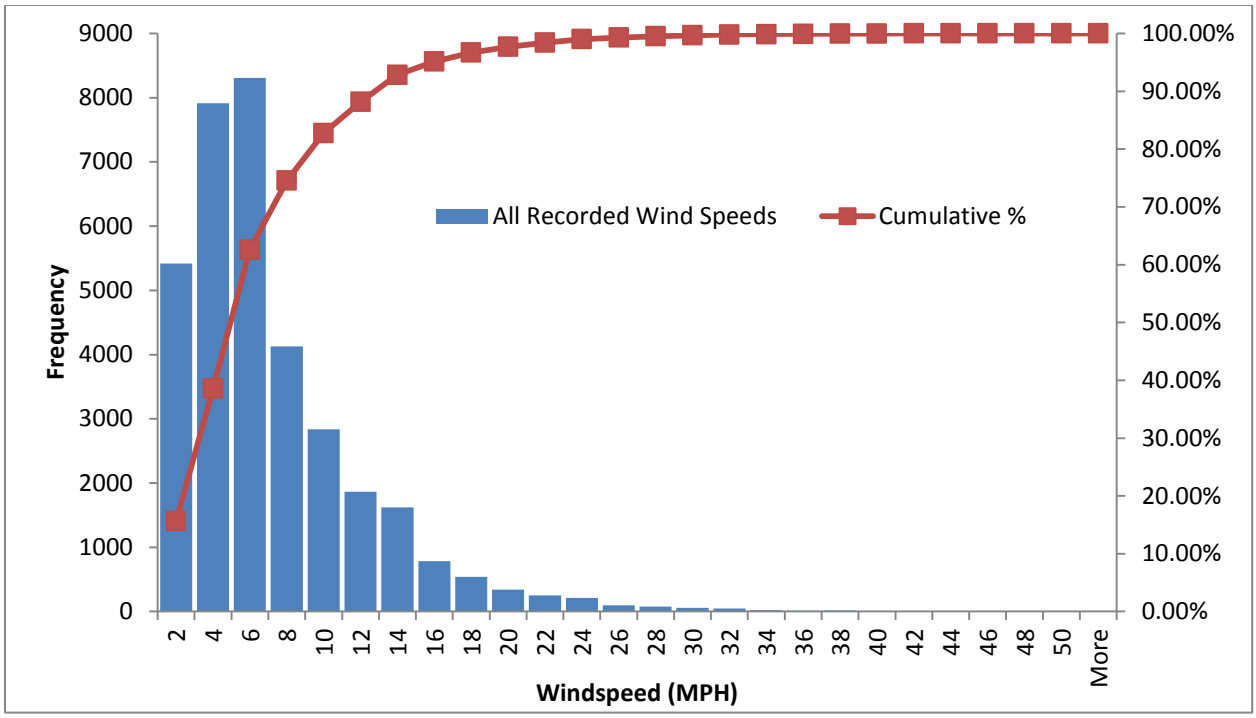


Figure 32: All Recorded Wind Speeds during the Period June 7 – 30, 2012

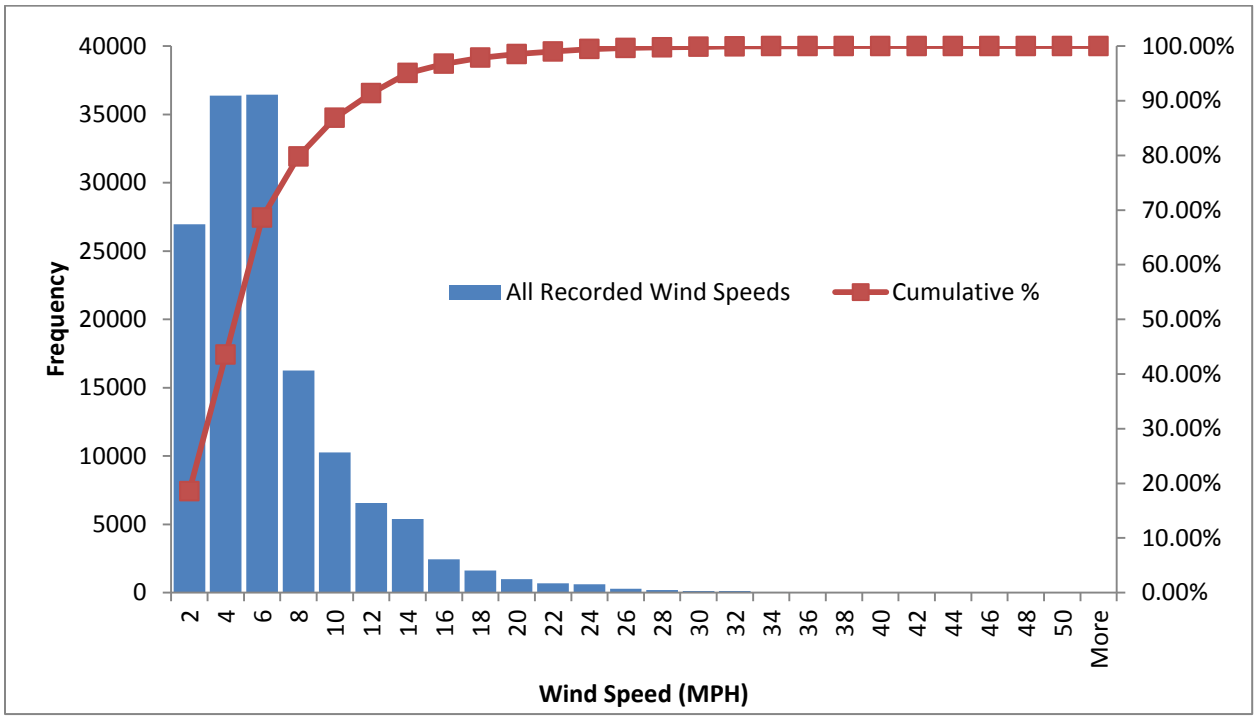


Figure 33: All Recorded Wind Speeds during the Nuisance Monitoring Period, July 1 – Oct 8

Comparing Figure 32 and Figure 33, the distribution of wind speeds is nearly identical, and yet the occurrence of unknown alarms is significantly different. Thus, it would appear that the high number of unknown alarms during the nuisance monitoring period is likely due to the poorly

installed sign. If we take this into account, then Table 6 could have potentially resembled the alarm rates in Table 7.

Table 7: MicroPoint Nuisance Sources with *Sign on Fence* Excluded from Data

Alarm Source	Alarms	NAR	UAR
Daytime			
Poor Camera Visibility[1]	2	0.02	----
High Winds	11	0.11	----
Unknown	48	----	0.49
sub total	61	0.13	0.49
Nighttime			
Poor Camera Visibility	55	0.56	----
Rain	30	0.30	----
Unknown	19	----	0.19
sub total	104	0.86	0.19
Total	165	0.99	0.68

Note 1: Refers to camera blooming during sunset condition

On average, the NAR and UAR are at an acceptable rate with the sign alarms filtered out. The other alarm events had similar wind distributions indicating that potentially other alarms could be due to the sign as well, but since there is no real evidence, further monitoring would need to be completed.

3.2.2.3 REDS Results

Due to limited funding, REDS was not tested independently, but was monitored during the testing of the other three sensors.

Table 8 contains the test results. Path 1 was approximately 5.5 ft from both REDS seismic sensors buried in the ground. Path 9 and 11 represented motion parallel to the seismic sensors at an approximate distance of 16 ft from the sensor. Paths 5, 6, and 7 were 45 degree motion toward the fence through the west-most seismic sensor. The paths were described previously in Figure 24.

In general REDS performed better against running versus walking adversaries. More testing needs to be conducted to form conclusions regarding the detection performance of vehicles.

Table 8: REDS Test Results

Approach	Distance (ft)	Path	Speed (ft/s)	Detections/ Repetitions	P_D @ 95% Confidence
Walk	125	1	5	5 / 10	22
Walk	125	9	5	22 / 30	57
Walk	81	5, 6, 7	5	18 / 30	43
Run	48	1	14	17 / 21	61
Run	125	11	19	29 / 30	85
Run	125	9	18	33 / 40	69
Run	81	5, 6, 7	15	26 / 26	89
Belly Crawl	18	1	1	35 / 35	92
Belly Crawl	71	9	1	7 / 8	53
Bear Crawl	18	1	1	0 / 20	0
Bear Crawl	71	9	1	0 / 8	0
Golf Cart	48	1	8	5 / 5	54
Polaris	48	1	13	8 / 10	49
Polaris, cont.	48	1	13	7 / 16	22
Minivan	48	1	15	4 / 4	46

Both the REDS footstep and vehicle sensor nodes tripped more unknown than known alarms. Table 9 contains the nuisance sources and alarm rate recorded for REDS footstep sensor nodes. The sensor test field does have periodic low-flying air traffic. The majority of traffic is due to low-flying jets versus low-flying helicopters. There is a road south of the barrier with light traffic (estimated 1 vehicle/hour during normal business hours) that is approximately 180 feet from the nearest seismic sensors connected to the sensor nodes. Observation during light vehicle traffic on the road did not show any triggered alarms. However, the test site sits proximal to an explosives test range, which undoubtedly caused several unknown alarms. The explosives test range conducts explosion tests periodically, sometimes multiple per day. REDS required periodic maintenance that left REDS incapable of relaying the nuisance data. Instead of the 98.8 days (2,371 hours) of monitoring, REDS had a total of 76.7 days (1841 hours) of nuisance monitoring.

No obvious correlation between alarm counts and weather data (wind speed, temperature, and humidity) was determined for the REDS footstep and vehicle sensor nodes. From observation, low-flying jets fly over the facility more often than low-flying helicopters. This, in addition to the explosion tests, may explain the high number of unknown alarms observed.

Table 10 contains the nuisance sources and alarm rate recorded for REDS vehicle sensor nodes. The number of unknown alarms was significantly larger than observed in the footstep sensor nodes. It is noted that the majority of the air traffic is low-flying jets versus low-flying helicopters.

Table 9: REDS Footstep Nuisance Sources and Alarm Rate

Alarm Source	Alarms	NAR	UAR
Daytime			
Unknown	125	----	1.63
sub total	125	0	1.63
Nighttime			
Unknown	7	----	0.09
Rain	8	0.10	----
Poor Camera Visibility	7	0.09	----
sub total	22	0.20	0.09
Total	147	0.20	1.72

Table 10: REDS Vehicle Nuisance Sources and Alarm Rate

Alarm Source	Alarms	NAR	UAR
Daytime			
Poor Camera Visibility[1]	8	0.10	----
Unknown	432	----	5.63
sub total	440	0.10	5.63
Nighttime			
Unknown	29	----	0.38
Rain	8	0.10	----
Poor Camera Visibility	53	0.69	----
Rabbit	1	0.01	----
sub total	91	0.81	0.38
Total	531	0.91	6.01

Note 1: Refers to camera blooming during sunset condition

3.2.2.4 VMD Results

Table 11 contains the test results for the VMD sensor. The sensor performed the best against walking intruders. It exhibited nearly the same results for runners with the exception of traveling on the 45 degree paths (2 through 7). The classification engine struggled to classify both the belly and bear crawlers. Increasing the contrast between the intruder and the background did improve belly crawling results but did not improve bear crawling results.

Table 11: VMD Test Results

Mode[1]	Approach	Distance (ft)	Path	Speed (ft/s)	Contrast[2]	Detections/ Repetitions	P_D @ 95% Confidence
Color	Walk	21	1	4	M	30 / 30	91
	Walk	81	5, 6, 7	4	L	28 / 30	80
	Walk	81	2, 3, 4	4	L	10 / 10	73
	Walk	125	11	4	L	30 / 30	91
	Walk	125	9	4	L	10 / 10	91
	Run	48	1	14	M	29 / 30	85
	Run	125	11	19	M	30 / 30	91
	Run	125	11	19	L	29 / 30	85
	Run	125	9	16	L	10 / 10	73
	Run	81	2, 3, 4	15	L	14 / 25	37
	Run	81	5, 6, 7	14	L	9 / 26	19
	Belly Crawl	18	1	1	M	4 / 30	5
	Belly Crawl	18	1	1	H	10 / 10	73
	Belly Crawl	71	9	1	M	3 / 8	11
	Bear Crawl	18	1	1	M	1 / 10	1
	Bear Crawl	18	1	1	H	1 / 10	0.5
	Bear Crawl	71	9	1	M	3 / 8	11
	Polaris, Cont.	48	1	13	—	3 / 16	5
	Polaris	48	1	13	—	0 / 5	0
	Run	81	5, 6, 7	15	L	10 / 10	73
Monochrome	Polaris	48	1	13	—	3 / 5	18
	Minivan	48	1	15	—	0 / 4	0
	Golf Cart	48	1	8	—	2 / 5	7
	Run	81	5, 6, 7	15	L	10 / 10	73

[1] Refers to the camera mode. The IR cut filter used in color mode is removed in monochrome mode.

[2] Refers to the intruder's contrast with respect to the background scene

It was noted that during the bear crawl tests with high contrast, after the test subject completed the travel path and stood up to return back to the starting location, the sensor alarmed nine out of the ten trials. This suggests that once the adversary approaches the barrier, they would need to remain low to the ground to bypass the sensor. The sensor performed poorly against vehicles approaching normal to the barrier (90 degree angle with respect to the barrier). Based on

observations, this is due to the size of the vehicle and limited time traveling through the field of view of the camera. The sensor was not able to classify the vehicle before it was in the rest position next to the barrier. The VMD sensor performed better when the vehicle traveled radially in or out of the field of view. Based on the results, the team decided to change the mode to monochrome to determine if this parameter affected performance. A brief set of run and vehicle tests were performed under the same conditions to compare the performance results (Appendix A.1.1). No detection difference was observed for the run tests; however, monochrome did perform better when comparing the Polaris vehicle test. The important note on the run tests is that the response time of the sensor was decreased in monochrome mode. That is the difference between the total time taken to complete the adversaries' path to the time when the sensor triggered an alarm. The average response time in monochrome mode was 230 ms, as opposed to 638 ms in color mode. Based on this observation and the improved vehicle tests, the team decided to leave the camera in monochrome mode for the system tests and nuisance alarm period. It is clear that more in-depth testing should be conducted to determine how monochrome mode handles the other adversary approaches.

As the nighttime illumination equipment was malfunctioning for most of the test period, the nighttime alarms were not assessed against the VMD system. The period of daytime was 53.7 days and was used in the calculation of the NAR. The breakdown of alarms by assessment category is shown in Table 12.

Table 12: VMD Nuisance Sources and Alarm Rate

Alarm Source	Alarms	NAR	UAR
Daytime			
Bird	1	0.02	----
Rabbit	15	0.28	----
Unknown	5	----	0.09
Total	21	0.30	0.09
Nighttime			
Rain	1	----	----
Poor Camera Visibility	16	----	----
Unknown	5	----	----

3.2.3 Individual Sensor Results Summary

Table 13 tabulates all the results from each of the sensors on the barrier to summarize the overall NAR for the system.

Table 13: Individual Sensor NAR/UAR Summary Results

Nuisance Summary	Photon	MicroPoint	REDS Footstep	REDS Vehicle	VMD	Total	Grand Total
Daytime Alarms	5	61	125	440	21	**652**	
Nighttime Alarms	6	104	22	91	----	**223**	**875**
NAR	0.11	0.99	0.20	0.91	0.30[1]	**2.13**[2]	
UAR	0	0.68	1.72	6.01	0.09[1]	**6.73**[2]	**8.86**

Note 1: VMD alarm totals and rates do not include nighttime periods in alarm rate calculation
Note 2: While the REDS system was only active for 76.7 days and the VMD system for 53.7 days, the Total alarm rates for the collective system were calculated over the entire 98.8 day test period to better represent total performance.

4 Integrated System Testing

4.1 System Test Methods

After characterizing each sensor against simple adversary behaviors, more complex methods were explored to attempt to bypass the entire system of sensors. The individual sensor characterization tests addressed detection on single-method approach paths to the barrier. However, a successful adversary will do more than simply approach the barrier. The ReKon system allows integration of multiple complementary sensors to combine their effectiveness. Thus, the integrated system testing will recreate actions necessary to bypass all the sensors, in an attempt to cross the barrier undetected. There are essentially six fundamental ways to cross the barrier: bridge over the barrier, tunnel under the barrier, climb over the fence, cut through the fence, travel through the maintenance access, or drive a vehicle through the barrier. The latter, a vehicle impact test, was not conducted during this effort. Based on the findings in Section 3.1.4, the monochrome mode was used for VMD during system testing, otherwise all other sensors were tested as configured during sensor characterization. The following tests were conducted for the system:

4.1.1 Bridging Attempts

All bridging attempts conducted without vehicles involved the subjects carrying a ladder to the barrier, then setting up and climbing the ladder to simulate a jump over the fence or Photon IR sensor. The vehicle tests involved driving close to the barrier, climbing to the roof, and simulating the actions of jumping over the fence. The list of tests conducted was as follows:

- Three walking subjects, cloaked with tarp (path 1)
- Three walking subjects, shoulder-to-shoulder (path 1)
- Three walking subjects cloaked with styrofoam door, shoulder-to-shoulder (path 1)
- Bear-crawling subject, dragging ladder (path 1)
- Drive golf cart (paths 1, 9)
- Drive Ford F-350 truck (paths 1, 9)

4.1.2 Tunneling Attempts

The test subjects used hand trowels to tunnel under the barrier, except in one attempt, where a shovel was used as noted. Although the soil at the test site is all compacted dirt, some of the tunneling tests were conducted on a loose soil condition by digging out a hole and backfilling with loose soil, to better approximate digging in sandy conditions. The list of tests conducted was as follows:

- Three walking subjects, cloaked with rigid tarp (stretched out taut to 8 ft x 10 ft), digging with shovel (path 1)
- Three bear-crawling subjects, cloaked with tarp (path 1)
- Three subjects walking in group (path 1)
- Bear-crawling subject (paths 1,8)

4.1.3 Climbing Attempts

The list of tests conducted was as follows:

- Walking subject climbs the fence on all fabric and pole locations noted

4.1.4 Cutting Attempts

The list of tests conducted was as follows:

- Walking subject cloaked with styrofoam door cuts through fence fabric
- Walking subject with backpack cut through fence fabric

4.1.5 Maintenance Access Attempts

The list of tests conducted was as follows:

- Walking subject
- Running subject
- Bear-crawling subject
- Belly-crawling subject

4.2 System Test Results

Table 14 summarizes the system testing results. The *System Detections/Repetitions* column scores a detection for a trial if even only one of the four sensors alarmed during the test attempt (as expected, LightLOC did not alarm at any point during these tests). The last four columns show how each sensor responded to each approach method. All personnel wore low-contrast clothing during system tests unless noted otherwise. On the Tunneling '*bear crawl, dig loose soil*' attempt on path 10, and on the Maintenance Access *'walk'* attempt, no results were recorded for REDS since the logging system failed. Technical difficulties also prohibited collection of REDS data during the Cutting '*walking with backpack'* attempt. The discrepancy in number of repetitions for the Maintenance Access '*run*' and '*belly crawl (M contrast)*' attempts were due to logging errors rendering the data unrecoverable.

Table 14: System Test Results

Method	Approach	Path	Speed (ft/s)	Distance (ft)	Dig Rate (in^3/s) / Duration (s)	System Detections/ Repetitions	MicroPoint Det./ Rep.	VMD Det/ Rep	REDS Det/ Rep	Photon Det/ Rep
Bridging	3 subjects walk w/ tarp	1	0.9	53	—	5 / 5	—	4 / 5	5 / 5	—
	3 subjects walk w/ tarp	1	5	53	—	2 / 2	—	2 / 2	2 / 2	—
	3 subjects walk abreast	1	1.3	45	—	2 / 2	—	2 / 2	2 / 2	—
	3 subjects walk abreast, w/ door	1	0.8	47	—	2 / 2	—	0 / 2	2 / 2	—
	Bear crawl	1	0.8	51	—	5 / 5	—	5 / 5	5 / 5	—
	Golf car, jump off roof	1	8.9	45	—	5 / 5	—	5 / 5	1 / 5	—
	Golf cart, jump off roof	9	10	69	—	3 / 3	—	3 / 3	1 / 3	—
	F-350, jump off roof	1	7.8	130	—	2 / 2	—	0 / 2	2 / 2	—
	F-350, jump off roof	9	7.8	130	—	3 / 3	—	3 / 3	3 / 3	—
Tunneling	3 subjects bear crawl w/ tarp, dig soil	1	0.5	46	1.2 / 300	2 / 2	—	0 / 2	2 / 2	—
	3 subjects, group walk, dig loose soil	1	0.8	46	4.3 / 80	3 / 3	—	3 / 3	3 / 3	—
	Bear crawl, dig soil	10	0.6	51	3.2 / 180	1 / 1	—	1 / 1	1 / 1	—
	Bear crawl, dig soil	8	0.6	51	2.7 / 180	1 / 1	—	1 / 1	1 / 1	—
	Bear crawl, dig loose soil	10	0.8	51	3.2 / 180	1 / 1	—	1 / 1	n/a	—
	Bear crawl, dig loose soil	8	0.7	51	2.7 / 180	1 / 1	—	1 / 1	0 / 1	—
	3 subjects walk w/ rigid tarp, dig soil w/ shovel	1	1.9	70	4 / 180	2 / 2	—	0 / 2	2 / 2	—
Climbing	Walk, climb fence	—	4	51	—	5 / 5	4 / 5	4 / 5	4 / 5	—
Cutting	Walk, cut fence	—	4	51	—	5 / 5	5 / 5	4 / 5	3 / 5	—
	Walk w/ backpack, cut fence	—	4	51	—	3 / 3	3 / 3	3 / 3	n/a	—
Maintenance Access	Walk	1	4	21	—	30 / 30	—	30 / 30	n/a	30 / 30
	Run	1	14	48	—	30 / 30	—	29 / 30	17 / 21	30 / 30
	Bear crawl (M contrast)	1	1	18	—	10 / 10	—	1 / 10	0 / 10	10 / 10
	Bear crawl (H contrast)	1	1	18	—	10 / 10	—	1 / 10	0 / 10	10 / 10
	Belly crawl (M contrast)	1	1	18	—	30 / 30	—	4 / 30	25 / 25	30 / 30
	Belly crawl (H contrast)	1	1	18	—	10 / 10	—	10 / 10	10 / 10	10 / 10

The system detected all bridging attempts. Once the adversary reaches the barrier, VMD is the only remaining sensor to be bypassed. VMD detected the subjects climbing the ladder as soon as the subject's body peaked the top of the ladder. It was observed that to confound the system, camouflaging methods would need to be incorporated into the bridging attempts. Results indicate the worst case for VMD detection is a large rigid surface used to disguise the adversary. During the '*3 subject walk w/ tarp*' attempt at 5 ft/s, it was noted that VMD did not alarm until the subject climbed the ladder and peaked the top; however, the REDS sensor detected them early in the approach, possibly due to increased noise generation coupled to the ground.

The system detected all tunneling attempts. REDS detected all attempts except the loose soil tests. VMD complemented most all the detections except during the '*bear crawl w/ tarp*' attempt, and when the tarp was stretched to 8 ft x 10 ft to increase rigidity, decreasing tarp movement. The other adversarial advantage to using any method where the subject is hidden by an object is that all additional movement after the adversary has reached the barrier is undetectable by VMD, unless some object loitering rule is implemented.

The system detected all climbing and cutting attempts. During one attempt, a backpack was used to simulate an adversary carrying tools to aide in the intrusion attempt, although results indicate the backpack does not reduce the VMD detection capabilities.

The system detected all maintenance access attempts. The bear crawl represents the worst case for both VMD and REDS, so the Photon IR is essentially the single line of detection for these attempts; however, the P_D of Photon IR is high, even on its own. VMD struggled to detect belly crawls, while REDS performed well against the belly crawls. In all the Maintenance Access attempts, Photon IR sensed all intrusions.

The methodology used to select the bypass methods used in the system testing was described in Section 4.1. The methods used to approach the barrier were based on the collective weaknesses of all the sensors. The sensor characterization results indicate that it is possible to bypass either REDS or VMD with the approach methods indicated to arrive at the fence, and, as mentioned previously, bridging or tunneling should be sufficient to bypass the MicroPoint or Photon IR. Thus, when the adversary reaches the barrier, it would be necessary to either bridge or tunnel since cutting the fence, climbing over the fence, or walking through the maintenance access are not advisable paths for covert conveyance. However, VMD and REDS collectively performed very well against the bridging and tunneling attacks, again confirming the importance of utilizing complementary sensors with line detection sensors. While there were weaknesses in several of the individual sensors, the ability to incorporate multiple complementary sensors enabled the integrated system to perform much better. Unfortunately, sufficient test data at the system level was not available at the time of this report to calculate P_D for direct comparison to the individual sensor performance, but a simple comparison of the "detections/repetitions" data is nonetheless illustrative. As previously mentioned, however, when a system simply involves adding several different sensors, the P_D may go up, but the NAR/UAR will certainly go up unless something is done to counter that. In the evaluation above, the system was considered successful if one sensor detected the subject. However, such a simple combination with no intelligence or filtering also results in counting each nuisance and unknown alarm from every sensor. Cumulating the results from Table 13, this would result in the integrated system having a high NAR of 2.13/day, but an even more egregious UAR of 6.73/day. This would typically be considered unacceptable for

high-security applications, and would tax the patience of the alarm monitoring personnel at any installation. While some measures could be taken to reduce this, such as correlating the assessment with the weather data, additional measures should be taken to reduce the NAR/UAR but still maintain acceptable detection performance

.

5 Sensor Fusion Demonstration

A primary objective of ReKon is to provision the barrier system with intelligent sensor fusion algorithms that can factor out nuisance and unknown alarms without diminishing the probability of detecting real alarms. It should be possible for a system with advanced sensor fusion software to exceed the detection performance of a conventional system in logical OR configuration because the powerful nuisance alarm filtering capability provided by sensor fusion will allow the sensors to be tuned to a greater level of sensitivity. A system without high performance sensor fusion software will be required to tune down the sensitivity of individual sensors until an acceptable compromise is found between nuisance activity and P_D. This compromise always provides an advantage to the adversary and it is the intention of ReKon to eliminate the need for that compromise so that the advantage is entirely pro-force.

Two approaches to sensor fusion were evaluated. The first approach used logical inference to fuse logic states output by the individual sensors by considering coincident events over a time window. This approach, which is also known as decision level or rule-based sensor fusion, is the most common method applied in the security industry today. The second approach applied statistical machine learning techniques to more detailed assessment data extracted from the sensors after the fact (except for VMD, this data is not made available by the other sensor vendors as part of their online communication protocols), along with one minute averaged weather data available from a local weather station.

5.1 Logical Inference Sensor Fusion

Most COTS security sensors on the market today provide a relay output to indicate a binary alarm state. All the sensors furnished on the barrier for this prototype use the relay interface as their defacto standard for integration into existing AC&D or Command and Control systems. Additionally, when a sensor does offer more sophisticated alternatives for data exchange, such as RS232 serial or IP, the information contained in that exchange still is reduced to little more than binary alarm state (and perhaps location). These conditions explain the current industry emphasis on logical inference as the sensor fusion methodology of choice, and also why it was the first approach undertaken during development of the ReKon prototype.

To implement Logical Inference Sensor Fusion, ReKon employs two main constructs: a holistic representation of system state referred to as the “Fact Base”, and a user scriptable set of rules that register to evaluate against the Fact Base when one or more fragments of the system state change. System state is composed of several layers. First there is the state of the individual line detection sensors: Photon, MicroPoint, and LightLoc. Next there is a layer of virtual sensors derived from the output of the VMD and REDS systems. Since both REDS and VMD report the presence of personnel or vehicles near the perimeter, the Fact Base has four virtual sensors to represent the combination of their states. If only one of REDS or VMD detect personnel the virtual MaybePerson sensor is activated; if both REDS and VMD detect personnel, the DefinitePerson sensor is activated. Likewise, if only one of REDS and VMD detect a vehicle, the MaybeVehicle sensor is activated; if both detect a vehicle, then the DefiniteVehicle sensor is activated. Both physical and virtual sensors also maintain memory of their previous state so that logic rules combining them can be evaluated with respect to a time window. Using a configurable time window allows the rules to account for synchronization differences between

sensor activations deriving from sensor placement and how rapidly individual sensors cycle between on/off states during a detection.

Multi-layered system state and configurable time windows allow for straightforward expression of any number of sensor fusion rules via logical inference. For the purpose of this evaluation, a rule was created to alarm on the coincidence of any alarm from Photon or MicroPoint with an active state in either MaybePerson or DefinitePerson within a 30 second time window. The rule would also alarm immediately if LightLoc alarmed since this sensor was deemed to have virtually non-existent NAR. This rule in effect combined the line of detection sensors with complementary volumetric sensing from VMD and REDS. Once the rule-based fusion alarm tripped, it would remain active until all underlying causes for the alarm have cleared, even if those causes weren't present when the alarm first activated. For instance, if MaybePerson and Photon alarmed, the rule would trigger, but then if MicroPoint alarmed, the fusion rule would not clear until Photon, MicroPoint, and MaybePerson have all cleared first.

5.2 Machine Learning Sensor Fusion

Subject matter experts at Sandia raised several objections regarding shortcomings in the logical inference approach to sensor fusion during design reviews. Most persuasive was the claim that logical inference will combine the weaknesses of the sensors as well as their strengths, producing a system that is overall easier to defeat. A survey of other fusion methods revealed several techniques from the field of machine learning that promised the ability to combine sensor data in accordance with learned probabilities. Using probabilistic decision boundaries allows the machine learning approach to avoid overruling a sensor when it is expressing high confidence in its detections, but also allows it to weigh corroborating evidence from other sensors when conditions matching lower confidence thresholds vulnerable to nuisance alarms are present.

Machine learning algorithms require an existing dataset to learn how to accomplish their tasks. This learning process is called training. It can involve data that is already classified with the labels the algorithm is supposed to learn (in our case, nuisance or true alarm), in which case it is referred to as supervised learning. Or, it can be given a set of unlabeled training data for which it can learn latent regularities on its own, which is referred to as unsupervised learning. There are also approaches that combine the two in various ways. In all cases, the quality and quantity of training data have a significant impact on the performance of the algorithm for its given task.

How much data a machine learning algorithm needs to train is an open question. The answer depends heavily on the choice of algorithm and the predictive power of the features in the dataset. A feature is defined as an individual measureable property of the phenomenon being observed. In the ReKon system, the phenomenon being observed is activity on and around the barrier, and the features include data reported by Photon, MicroPoint, REDS, VMD, and weather. These sensors all provided some data in addition to alarm state. Photon provides the logic state for each beam on the vertical bar, giving some indication of the height of the object. MicroPoint provides the amplitude under or over threshold for each event detected along with cell location on the perimeter. REDS only provided an on/off state for footstep and vehicle detections. VMD provides a rich real-time metadata stream that includes object classification (human, vehicle, or other), confidence coefficient between 0 and 1 for the object classification, and approximate pixel location. The weather provides one minute averages for wind speed, wind

direction, temperature, humidity, and rain. Unfortunately, as is commonplace in the industry, the MicroPoint and Photon vendors do not support harvesting the additional sensor data in real-time. The data was instead extracted from log files generated by vendor software after the fact. As a result, the machine learning algorithm and analysis had to be performed offline.

The training data can be simulated as well as collected from real world events. When simulated, the data is created from prior knowledge of the task the algorithm will be accomplishing and the natural range of its data inputs. Similar to how children prepare for real life in the simulated learning environment of school, it is not uncommon for a machine learning algorithm to receive simulated training to classify data that would be too dangerous, costly or time consuming to acquire in the real world. Also like a person, machine learning algorithms can keep learning once deployed by using feedback about the accuracy of its predictions to continuously refine its performance.

5.3 Data Capture and Data Overview

Since training a machine learning algorithm requires the acquisition of sufficient sample data, several data capture programs were used to accumulate event data for the five-month period from early May 2012 to early October 2012. For live data entering and exiting the ReKon system, this task was simplified by the presence of a logging and auditing service that can record any messages matching a pattern to a persistent database. Logging and auditing all activities from Photon, MicroPoint, REDS, and VMD, as well as events from the Complex Event Processor, state changes from the Rule Engine and logical inference alarm events generated approximately 177MB of archived data. Live data from Photon, MicroPoint, and REDS included alarm active and clear events generated by each sensor's relay outputs. The VMD offers an event notification API that sent detailed XML reports about each alarm event to web service endpoints hosted by ReKon. Although both Photon IR and MicroPoint generate extra diagnostic data along with each alarm event, neither provides online, programmatic access to that data. However, each system provides software that is able to display the diagnostic data, allowing a batch extraction strategy to be contrived granting non-realtime access to the data. This data was compiled into files resulting in an additional 65MB of diagnostic data from Photon IR, and 968K from MicroPoint. Sandia was also able to provide one minute average weather data from a nearby weather station for the five month period adding 20MB of data.

Every event involving Photon and MicroPoint was manually classified as either a real or nuisance alarm by staff at Stonewater Control Systems after reviewing video footage of the event. These assessments were then cross-referenced with the separate assessments performed by Sandia staff for events captured by the NADS. The verified assessments and approximately 261MB of sensor data were then cross-correlated to produce two data files. The first file contained data that allowed assessment of the logical inference sensor fusion system with respect to the performance of the individual sensors in the system. Correlation of logical inference alarms with individual sensor alarms primarily helped to determine real alarms that logical inference failed to report. Logical inference alarms were also matched to the manual event classifications assigned to the alarm rule's component sensors, enabling calculation of performance metrics for the overall logical inference method (P_D, NAR, and UAR).

The second file contained features correlated from each sensor for every event generated by the Photon or MicroPoint sensors. These features were used for training and evaluating machine learning algorithms. The file contains one record for each event, with each record containing rich data acquired from Photon, MicroPoint, VMD, and weather; footstep and vehicle detection status from REDS; and precise timestamp, index, and classification label. To account for time synchronization and sensor placement variances in event response from each sensor, each record was compiled by accumulating VMD and REDS data from a window starting 15 seconds before and ending 15 seconds after events detected by Photon or MicroPoint. Weather was already provided in one minute intervals so each record incorporated the weather data nearest to the Photon or MicroPoint event timestamp. Records were generated for all events without discriminating for maintenance activity or any sensor downtime. If a pedestrian or vehicle was identified as causing the event, it was marked as a real alarm. Otherwise it was marked as a nuisance alarm. If a sensor was down for a particular event, data signifying non-detection for that particular sensor was assigned to that event. Table 15 summarizes the distribution of data as it applies to the primary event sources.

Table 15: Machine Learning Event Distribution

Sensor	Real Alarms	Nuisance Alarms	Total
ALL	767	1046	1813
MicroPoint	226	1017	1243
Photon	541	29	570

A deeper look at the data distribution as it pertains to complementary sensors (VMD, REDS) shows uneven participation by both across all event types. Since individual component testing concluded that both the VMD and REDS sensors had a relatively low P_D for some approach methods, inconsistent contributions represent likely real-world performance and provides confidence that the reported results transfer to expected conditions in a real-world environment. Table 16 documents the allocation of REDS and VMD data for real and nuisance alarms in the dataset.

Table 16: Machine Learning Event Distribution for Secondary Sensors

Sensor / Status	Real Alarms	Nuisance Alarms	Total
REDS Footsteps Present	489	13	502
REDS Footsteps Absent	278	1033	1311
REDS Vehicle Present	279	17	296
REDS Vehicle Absent	488	1029	1517
VMD Present	694	61	755
VMD Absent	73	985	1058

The data in Table 16 reveals that REDS footsteps were present for about 64% of the real alarms, and VMD detected at some threshold for approximately 90% of the real alarms. Both sensors participated in nuisance alarms, but at extremely low rates (1.2% for REDS footstep, and near 6% for VMD). In the interest of full disclosure, events captured in the machine learning dataset include alarms generated by routine maintenance during which staff were stationary at the barrier (and therefore undetectable to REDS), or obscured from the camera on the safe side of the

barrier (and therefore undetectable to VMD). Although these sensors both have a fairly low P_D, the statistics presented above might represent lower than expected performance due to the inclusion of these records. The decision was made to retain these records precisely because the lower P_D of the sensors renders them more susceptible to defeat. As such, events mimicking this defeat were valued for providing more realistic evidence of how the machine learning system would perform under adverse conditions or against a capable adversary. Overall, gaps and other inconsistencies in the secondary sensor data demonstrate that there is no straightforward logic expression that can combine data from both the primary and complementary sensors to produce an accurate alarm classification in all cases. Under ideal circumstances there is a high probability that all sensors will report on a true alarm, but there is a significant number of cases where they will not. The data contained in the machine learning dataset approximates these less-than-ideal conditions.

The amount of data in the machine learning data set (1813 records) is quite small for a fairly complex classification task. Additionally, training and evaluating the performance of the algorithms involves randomizing the data and breaking it down into even smaller segments for training, tuning, and testing. Also, certain tests required moving all instances of a certain pattern of activity from the training set to the test set (e.g., bear crawl and belly crawl). These requirements created conditions in which records in the test set had no analog in the training set. Such a split often occurs in real world machine learning development, and the recognized solution is to synthesize data that generalizes the missing pattern of activity and include it in the training set. To account for the most egregious examples of missing data (bear crawl, belly crawl, and flapping sign (see Section 3.2.2.2)), 21 additional data records, a 1% increase, were synthesized to provide extra learning material. Although this is a negligible amount, results will be presented with and without the synthesized data.

5.4 Sensor Fusion Analysis

The following statistics were computed to measure the effectiveness of the logical inference and machine learning approach to sensor fusion:

- *True Positives*: count of real alarms predicted as real alarms
- *False Positives*: count of nuisance alarms predicted as real alarms
- *False Negative*: count of real alarms predicted as nuisance alarms
- *True Negatives*: count of nuisance alarms predicted as nuisance alarms
- *Precision*: % alarm predictions that were correct

$$\frac{True\ Positives}{True\ Positives + False\ Positives}$$

- *Recall*: % real alarms properly classified as real alarms

$$\frac{True\ Positives}{True\ Positives + False\ Negatives}$$

- *Specificity*: % nuisance alarms properly classified as nuisance alarms

$$\frac{True\ Negatives}{True\ Negatives + False\ Positives}$$

- F1 Score: weighted average of precision and recall (harmonic mean)

$$\frac{2 * precision * recall}{precision + recall}$$

These metrics were used to evaluate both logical inference and machine learning sensor fusion for four different test scenarios. The first scenario calculates the P_D for logical inference and machine learning for trials testing Photon and MicroPoint. This will allow direct comparison with the conventional system benchmarks documented in Section 3.2 of this report. The data in Table 17 and Table 18 present results for Photon that can be compared to Table 3.

Table 17: Machine Learning Photon Test Results

Approach	Path	Speed (ft/s)	Detections/ Repetitions	P_D @ 95% Confidence
Walk	1	4	30 / 30	91
Belly Crawl	1	1	40 / 40	93
Bear Crawl	1	1	20 / 20	86
Run	9	14	30 / 30	91

Table 18: Logical Inference Photon Test Results

Approach	Path	Speed (ft/s)	Detections/ Repetitions	P_D @ 95% Confidence
Walk	1	4	30 / 30	91
Belly Crawl	1	1	25 / 40	48
Bear Crawl	1	1	0 / 20	0
Run	9	14	30 / 30	91

As the Logical Inference results show, the tests presented several challenges to achieving accurate prediction for sensor fusion. First, the REDS sensor malfunctioned for one full day of testing which encompassed all of the walk tests and a portion of the belly crawl tests. Fortunately the VMD system provided strong detection for all the walk tests which allowed the Logical Inference approach to compensate for REDS absence (remember that either REDS or VMD can generate a MaybePerson virtual alarm, which creates an inference alarm when combined with Photon or MicroPoint). However, VMD encountered serious difficulty discerning a crawling subject, failing to report for most of the belly and bear crawl tests. When REDS was restored to proper functioning, it was able to pick up most of the belly crawls, but failed for all of the bear crawls. These failures reinforce the concept that logical inference based sensor fusion combines the weakness of the sensors to produce a system that is overall easier to defeat than a system without such fusion.

In contrast, the Machine Learning results are on a par with the conventional system results. Despite malfunction and poor performance from contributing sensors, machine learning was able to learn a probability distribution over the data that could accurately distinguish real alarms in conditions that foil traditional sensor fusion methods. The algorithm did require some synthetic data to discern the belly crawl tests that occurred when REDS was malfunctioning. The test set contained the only instances of this unique circumstance in the dataset, and the only other events close to it were obvious nuisance alarms caused by rabbits. Without the synthetic data, the machine learning would not have had examples to learn to separate the belly crawls from the other nuisance alarms. Table 19 presents the test results with the synthetic data excluded.

Table 19: Machine Learning Photon Results without Synthetic Training Data

Approach	Path	Speed (ft/s)	Detections/ Repetitions	P_D @ 95% Confidence
Walk	1	4	30 / 30	91
Belly Crawl	1	1	34 / 40	72
Bear Crawl	1	1	20 / 20	86
Run	9	14	30 / 30	91

The machine learning was still intelligent enough to pick up all of the bear crawl events that consistently thwarted detection by REDS, VMD, and the logical inference system. As mentioned previously, the belly crawl events that it missed had no counterpart outside of the test set except a few nuisance alarms by rabbits. The addition of four synthetic events provided enough reinforcement that the learning algorithm could consistently distinguish attacks from relatively similar nuisances.

Table 20 and Table 21 present data comparable to the MicroPoint test data presented in Table 5.

Table 20: Machine Learning MicroPoint Test Results

Approach	Location	Detections/ Repetitions	P_D @ 95% Confidence
Climb	On Poles	30 / 30	91
Climb	Between Poles	30 / 30	91
Cut	Between Poles	26 / 30	72

Table 21: Logical Inference MicroPoint Test Results

Approach	Location	Detections/ Repetitions	P_D @ 95% Confidence
Climb	On Poles	20 / 30	50
Climb	Between Poles	28 / 30	80
Cut	Between Poles	11 / 30	22

The results demonstrate again how logical inference rule-based systems fail to be reliable in the face of inconsistent sensor performance. Unfortunately, many of the MicroPoint tests were performed in quick succession without moving away from the barrier. The VMD struggled to

identify targets when they overlapped the pixel location of the barrier in the video image. Without the test subject stepping away from the barrier between tests, neither REDS nor VMD could reliably detect a human presence. The machine learning was consistently able to learn a decision boundary that accounted for these performance gaps. The one set of tests where it achieved lower accuracy involved cuts on the fence that terminated as soon as MicroPoint triggered instead of continuing through to the recommended number of eight cuts per attack. A cluster of eight closely packed events would likely have given enough information to the machine learning algorithm to look beyond the relatively low amplitude of the cuts reported by MicroPoint. Without the extra information, the closest matching event patterns in the dataset were low amplitude nuisance alarms caused by wind. Synthetic data representing the abridged fence cut events as real alarms had the effect of turning the previously eliminated nuisance alarms caused by wind back in to actual nuisance alarms. Although these abnormal attack attempts would not have yielded an opening sufficient to breach the fence, examining the test conditions here yields useful insight: since both REDS and VMD have a fairly low P_D (for some approaches), they are susceptible to defeat by a capable adversary, so the machine learning algorithm must be able to detect attempts to cut through the fence without corroborating data from the secondary sensors. To detect fence cuts, the machine learning algorithm will require more detailed event data that captures multiple low-amplitude cuts in rapid succession, which the MicroPoint currently does not provide.

The purpose of the second test scenario was to assess the NAR experienced by both sensor fusion methods for the 100 days of passive testing from July 1 to October 8. This scenario provides data for comparison to the reported NAR for the conventional system for the same time period. Table 22 describes the manually assigned classifications for the data subset used for the nuisance alarm analysis for machine learning and logical inference.

Table 22: Assigned Event Classification for Machine Learning and Logical Inference Passive Testing Datasets

	Classified Real	Classified Nuisance	Total
Machine Learning	127	780	907
Logical Inference	140	779	919

The difference in alarm counts between Machine Learning and Logical Inference results from a misconfiguration in the Photon data capture software that occurred twice after a Windows update resulted in a reboot. The Logical Inference dataset includes those alarms because it recorded live data from alarm relays that were reported to the ReKon system. Fortunately, during that time period no nuisance alarms occurred, only maintenance activity that has been classified as "real" because human activity triggered the alarms. For machine learning, the training set included all records with a timestamp before July 1 plus the 21 synthetic data records used in the previous test scenario. The test data for which the scores are reported include all records with a timestamp greater than June 30 and less than October 9. Results will also be presented without the synthetic training records. For logical inference the dataset was filtered so that any alarms occurring within 30 seconds of another were combined to count as one. This same processing was applied to the conventional system dataset for the passive testing analysis. The machine learning dataset did not undergo the same processing because it was able to achieve high accuracy without it. Table 23 displays the results for the passive testing period.

Table 23: Sensor Fusion Results for Passive Testing Phase

	Recall	Precision	Specificity	F1	True Positive	False Positive	True Negative	False Negative
Machine Learning	1.0	.985	.997	.992	127	2	778	0
Logical Inference	.82	.92	.987	.867	116	10	769	24

The results provide an impressive example of the benefits offered by the machine learning approach to sensor fusion. Most importantly, the machine learning algorithm correctly classified every event on the barrier that had a human cause. As mentioned previously, a major flaw of logical inference is that it reduces the overall capability of the system by combining sensors' weaknesses as well as their strengths. The machine learning approach shows there is a way beyond this dilemma. Additionally, of the 780 nuisance alarms recorded in the dataset, machine learning correctly classified all but two as nuisances. Examination of those two events shows they were both caused by rabbits loitering in the maintenance access for a period of several seconds. Since this event signature matches the signature of a belly or bear crawling adversary that has defeated both REDS and VMD, classifying the events as true alarms is an acceptable tradeoff for protection against the more damaging security breech. The logical inference results support the claim that this approach to sensor fusion achieves its ability to reduce the NAR through a corresponding reduction in detection capability. Although precision and specificity were admirably high, recall suffered a significant drop, proving that the overall security of the system has been diminished.

Table 24 displays the results for the passive testing period for machine learning without the advantage of synthetic training data.

Table 24: Machine Learning Results without Synthetic Training Data for Passive Testing Phase

	Recall	Precision	Specificity	F1	True Positive	False Positive	True Negative	False Negative
Machine Learning	.921	.959	.994	.939	117	5	775	10

Without the synthetic data the machine learning scores drop a noticeable amount but still remain high. The largest change is in recall, mostly because a number of system tests occurred after July 1 that have no analogue in the training data set. These tests involved concerted efforts to defeat the system by exploiting known weaknesses in the barrier's sensor configuration. Most of these attacks involved obscuring attackers behind some kind of camouflage to prevent VMD detection and then executing one simulated cut on the fence that produced a low amplitude signal to MicroPoint. However, generating a small number of representative training events allowed it to learn the proper classification, as shown in Table 25.

The third test scenario evaluated the results of both sensor fusion algorithms on attacks devised for the system level testing. The attacks in the system level tests represent an increase in difficulty because they were designed to exploit known weaknesses in individual component

sensors. Only the subset of system level attacks presented in section 4.2 that involved Photon or MicroPoint are relevant to this analysis.

Table 25: Sensor Fusion Performance on System Level Testing

Method	Approach	Logical Inference	Machine Learning
Climbing	Walk, climb fence	4 / 5	4 / 5
Cutting	Walk, cut fence	5 / 5	5 / 5
	Walk w/ backpack, cut fence	3 / 3	3 / 3
Maintenance Access	Walk	30 / 30	30 / 30
	Run	30 / 30	30 / 30
	Bear Crawl	0 / 20	20 / 20
	Belly Crawl	25 / 40	40 / 40

The evidence presented above supports the conclusion that logical inference will have a difficult time defending against a sophisticated adversary who knows how to exploit the weakest sensor in the system. Machine learning does not suffer from this same defect. The trial that machine learning did not identify involved a climb on the fence that the MicroPoint sensor did not report. Combined with the difficulty that the VMD system had identifying targets overlapping the fence structure in the field of view, there was just simply not enough data in the system to identify this attack. Enhancing the system to detect this attack is straightforward: improve the VMD to ignore static background features such as the barrier structure, simplifying the identification of occluded targets, and incorporate a ground sensor that exports more than just an alarm state, thus making it a suitable candidate for machine learning fusion. Additionally, MicroPoint only provides data once a threshold has been breached. If MicroPoint always provided data for every stimulus, there would have been information available for the algorithm to use in its decision-making process. Unfortunately for this isolated case, there was no information available.

The fourth test scenario was developed with two main goals in mind: one, provide a more general assessment of the machine learning performance over all the data in the dataset; and two, perform a sensitivity analysis to determine how the test scores change as sensors are added and removed. As discussed previously, training and testing the machine learning algorithm involves randomizing the entire dataset, and then dividing respectively by 60%/40% for the already small dataset into training and test subsets. The accuracy of the algorithm varies by how well the training data reflects the test data and also by how many of the most difficult examples get excluded from the score by ending up in the training set. A better picture of the algorithms performance can be obtained by running 200 randomized trials and calculating the score at a 95% confidence interval. The randomized trials were performed on the complete dataset, and also on every other permutation of sensors considered by the algorithm to provide the sensitivity analysis. Figure 34 and Table 26 show the results of this test scenario for machine learning with the 21 synthetic training events included.

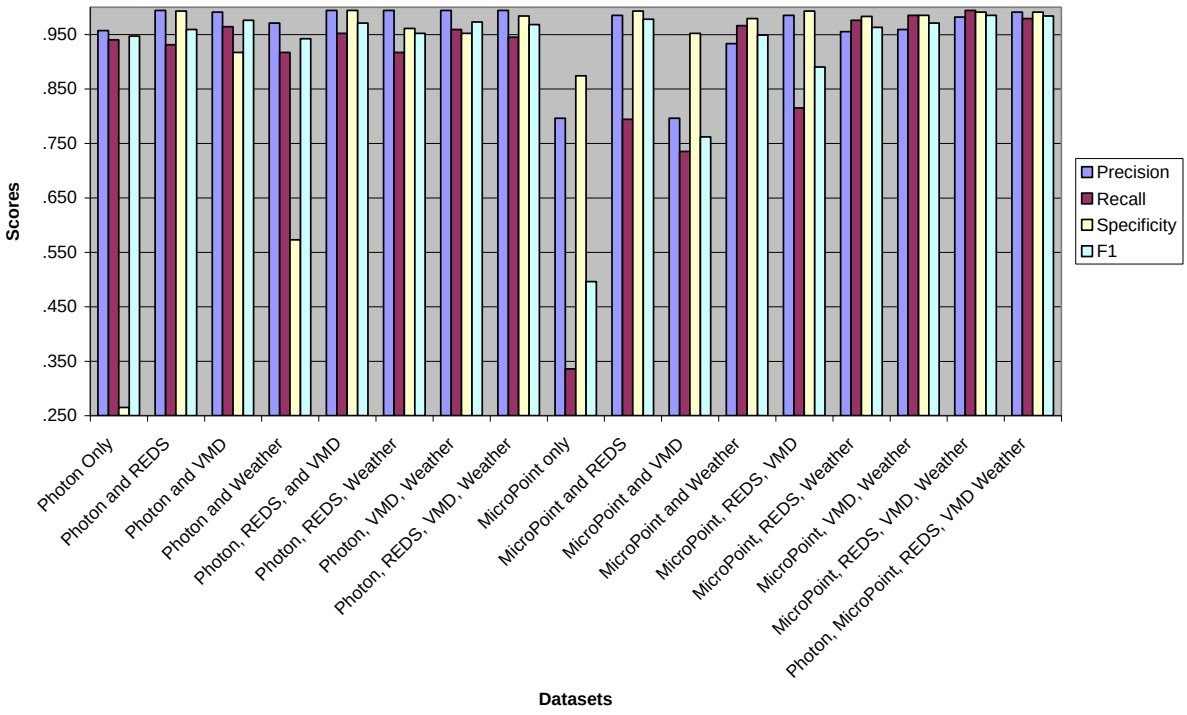


Figure 34: Machine Learning Sensor Fusion Results @95% Confidence, 200 Trials

Table 26: Machine Learning Sensor Fusion Results @95% Confidence, 200 Trials

Dataset	Precision (%)	Recall (%)	Specificity (%)	F1 (%)
Photon Only	95.7	94.0	26.5	94.7
Photon and REDS	99.4	93.1	99.3	95.9
Photon and VMD	99.1	96.4	91.7	97.6
Photon and Weather	97.1	91.7	57.3	94.2
Photon, REDS, and VMD	99.4	95.2	99.4	97.1
Photon, REDS, and Weather	99.4	91.7	96.1	95.2
Photon, VMD, and Weather	99.4	95.9	95.2	97.3
Photon, VMD, REDS, and Weather	99.4	94.5	98.4	96.8
MicroPoint Only	79.6	33.6	87.4	49.6
MicroPoint and REDS	98.5	79.4	99.3	87.9
MicroPoint and VMD	79.6	73.5	95.2	76.2
MicroPoint and Weather	93.3	96.6	97.9	94.9
MicroPoint, REDS, and VMD	98.5	81.5	99.3	89.0
MicroPoint, REDS, and Weather	95.5	97.6	98.3	96.3
MicroPoint, VMD, and Weather	95.9	98.5	98.5	97.1
MicroPoint, REDS, VMD, and Weather	98.2	99.4	99.1	98.5
Photon, MicroPoint, REDS, VMD, and Weather	99.1	97.9	99.1	98.4

The logical inference sensor fusion results for the overall test period are presented separately because the trial was run live and only once.

Table 27: Logical Inference Sensor Fusion Results

Dataset	Precision (%)	Recall (%)	Specificity (%)	F1 (%)
Logical Inference	94.0	81.8	96.2	87.5

The results listed in Table 27 again reinforce the obvious weaknesses in sensor fusion using logical inference as well as demonstrate the significant promise of the application of machine learning to the problem domain. For both tests, the results are skewed somewhat by the absence of some sensor data due to equipment malfunction, but it is clear that machine learning offers significantly more resilience in the face of sensor loss or defeat. The test data was not scrubbed for records that could be deemed questionable, such as events that are consistently false negative even though they are bracketed on both sides by positive identifications a few seconds apart (this

would happen when large groups of people were inspecting the fence), or when the barrier sensors were undergoing maintenance and would have normally been placed into access mode. For the machine learning experiment, most if not all the false negatives can be accounted for by these circumstances. However, any sensor fusion system for perimeter security clearly should sacrifice precision for recall when tuning the algorithm. Since a large perimeter will obviously have vastly more fence line than maintenance access gates, the most important dataset in the machine learning sensor fusion results is the one for "MicroPoint, REDS, VMD, and Weather". This configuration achieves 99.4% recall, including cut tests which stopped short of the recommended number of cuts as well as many other instances in which REDS and VMD were unable to detect human presence. At the same time, the machine learning was able to eliminate over 99% of nuisance alarms for the same dataset over the test period. The scores for logical inference show that while it was able to meaningfully reduce nuisance alarms, eliminating 96.2%, it was only able to do this at the cost of dramatically lower recall (81.8%)

The machine learning sensitivity analysis reveals that the largest contributors to correct nuisance classification (specificity) are the VMD for Photon IR, and weather for MicroPoint. Largely this is because these sensors provide the most detailed stream of information. REDS provided significant improvement to the effectiveness of machine learning with the Photon IR dataset, but since REDS provides only truth state values regarding detection, its contribution was overshadowed by that of VMD. Similarly, the combination of weather data with MicroPoint proved so effective there was little room for REDS to make a contribution with the limited data it provides. Overall, machine learning displayed outstanding results with the ability to correctly classify 99% of the nuisance alarms with the best sensor combinations, and still maintain excellent recall for true alarms. Correct classification of nuisance alarms enables the system with multiple options, such as forwarding them to the alarm station labeled as nuisance or lower priority, or not forwarding them at all, depending on the security policies in place. Most if not all false negatives can be explained by sensor malfunction, situations with other alarms already present, or the system undergoing maintenance.

An interesting insight can be drawn from the performance differences between both Photon and MicroPoint when combined separately with REDS and VMD. The combination of Photon and VMD outperforms the combination of Photon with REDS. However, with MicroPoint the opposite is true. This highlights the difficulty experienced by VMD distinguishing targets overlapping the fence on the image. Efforts to improve the VMD system's performance in this area would undoubtedly yield higher scores when fusing MicroPoint and VMD together.

Results for test scenario three machine learning sensor fusion without any synthetic training data are presented in Table 28.

Table 28: Machine Learning Sensor Fusion Results @95% Confidence, 200 Trials, No Synthetic Training Data

Dataset	Precision (%)	Recall (%)	Specificity (%)	F1 (%)
Photon Only	94.9	93	36.1	93.5
Photon and REDS	98.1	80.4	82.9	87.7
Photon and VMD	98.4	94.7	96.0	96.3
Photon and Weather	96.6	89.4	60.5	92.9
Photon, REDS, and VMD	98.7	93.0	90.6	95.8
Photon, REDS, and Weather	98.7	89.4	91.5	93.0
Photon, VMD, and Weather	99.0	93.8	92.4	96.1
Photon, VMD, REDS, and Weather	99.0	92.2	92.9	95.2
MicroPoint Only	78.0	33.1	97.1	47.0
MicroPoint and REDS	93.5	73.1	98.2	82.3
MicroPoint and VMD	77.8	70.8	94.7	74.3
MicroPoint and Weather	93.1	95.6	97.9	94.5
MicroPoint, REDS, and VMD	93.1	75.8	98.1	83.4
MicroPoint, REDS, and Weather	94.9	96.3	98.4	95.6
MicroPoint, VMD, and Weather	95.2	96.6	98.4	95.8
MicroPoint, REDS, VMD, and Weather	96.9	97.1	98.7	97.1
Photon, MicroPoint, REDS, VMD, and Weather	97.9	96.6	98.2	97.1

The scores without synthetic training are only marginally lower than the scores with it. Recall for the best case combination of sensors (MicroPoint, REDS, VMD, and Weather) dropped a little more than 2%, and specificity dropped a little less than 1%. These results show that the algorithm was already learning quite well even though the number of training records is relatively small for the problem being solved. Also, the source data was generated without any forethought applied as to the requirements of training a machine learning algorithm, resulting in many difficult corner cases having only limited number of examples, examples which were often barely distinguishable from known nuisance alarm sources. These circumstances suggest that more emphasis on analysis and the methodical generation of training cases provide an opportunity for even greater improvements in the reported results.

Although the machine learning approach was evaluated with offline datasets, this was only done because the required data could not be extracted from the sensors in real-time. If the sensors did provide this information live, then it would have been a simple exercise to add a machine learning prediction service to the existing software architecture. The Complex Event Processor

already supports aggregating and transforming multiple sensor feeds into new data formats, which can be published for processing by the prediction service. In fact, it is envisioned that machine learning prediction will be just one facet of a multi-layered approach to the NAR reduction that will combine heuristics, statistical analysis and logical inference to reduce the likelihood of false negatives. The ReKon™ software architecture was developed to make the expression of such concepts straightforward through service composition.

The results of our sensor fusion analysis show promising advantages to be gained by applying machine learning to multi-sensor intrusion detection systems. At the same time, the analysis demonstrates that rule-based logical inference sensor fusion is too simple to handle sensors with inconsistent detection performance across a range of threat scenarios, which results in a system that is far less capable than one in which each sensor is evaluated independently. In the first three test scenarios (individual sensor characterization for Photon and MicroPoint, Long-term NAR analysis, and aggressive system level testing), machine learning displayed an ability to reason accurately about the source of an alarm even when one or more sensors were defeated or malfunctioning. The defeats that machine learning did experience were largely the result of insufficient information provided by the sensor manufacturers. Except for the VMD system, the sensors assembled for this project only report data after an alarm threshold has been breached. Using sensors that offer more data at higher frequency will allow the machine learning algorithms to draw increasingly accurate decision boundaries between nuisance and real alarm events, all but eliminating the few corner cases discovered in the course of testing. Without sensor fusion, the increased detection performance gained from deploying additional sensors on the perimeter is overwhelmed by the increase in NAR, rendering the system unusable. As our long term NAR analysis results show, machine learning was able to eliminate all but two nuisance alarms for the 100-day period, and those nuisance alarms matched exactly the signature of a bear crawling intruder who has defeated the VMD and ground sensors to penetrate the maintenance access. Without the attendant decrease in detection capability that accompanies other sensor fusion alternatives, customers who equip their perimeters with multi-sensor machine learning fusion algorithms will no longer have to sacrifice P_D to obtain acceptable NAR. Intelligent cooperation between sensors in a multi-sensor intrusion detection system promises to be the next generation advance in perimeter security, and these tests document the real benefits machine learning can offer in achieving such cooperation.

6 Conclusion and Recommendations

The security world is advancing, and a need exists for a new type of perimeter security that integrates intelligent detection with assessment and delay. An ideal system would permit integration of varied sensor phenomenologies, and allow for modular construction to expedite deployment and reduce cost. It would be scalable to integrate well with both large and small sites. Additionally, it should be configurable to allow the system to be tailored to the specific performance and security needs of a specific site. The ReKon system has been demonstrated, which meet these goals through integration of various types of detection and assessment inputs on virtually any physical barrier, and incorporation of advanced algorithms to provide enhanced data fusion.

A suite of complementary and disparate sensors was implemented on this prototype to highlight the effectiveness of complementary sensing, and to evaluate the systems' ability to incorporate various input types. The capability exists for the sensor suite to be customized to the needs of a particular installation, whether the threats of concern consist of vehicles, personnel, aerial, underground, or a combination of all. Whichever sensors are chosen, an effective perimeter will use complementary sensor technologies to allow complete coverage of the assessed threat definition, overcome individual sensor weaknesses, and combine their strengths.

The prototype was built on the MNB with integrated camera towers and fencing, which allowed for modular construction and reduced on-site installation time. The software and electronics hardware architecture of ReKon is also modular, allowing the detection and assessment functions to be abstracted from the barrier, such that integration with any other type of barrier is permissible. Additionally, the scalable features in ReKon allow the system to be expanded with additional hardware to increase the perimeter distance or increase the detection capabilities if needed. It is also able to incorporate the latest cyber security standards, and permits configuring the system to the unique security needs of each site. The modularity, scalability, and configurability allow ReKon to be customized to provide the most secure solution matching the requirements of each site.

A common drawback of a system that can incorporate multiple sensors to provide adequate delay would normally be substantially increased NAR over a single-sensor solution. In the performance testing of the ReKon system, the ability of the system in a conventional configuration (logical 'OR' combination of sensors) to detect each attack was demonstrated with success. The individual sensors were characterized, and the weaknesses of each sensor were exploited in designing attempts to bypass the entire system. These included running through Photon, climbing the fence, attempting to bypass the fence by ladder or by digging under, and involved the use of obscuration techniques and vehicles. All were successfully detected by at least one of the sensors. As expected, the increased detection capability came at a cost of very high NAR when the sensors were evaluated in this simple configuration. Results were presented which compared and contrasted the performance of this conventional system with more advanced sensor fusion techniques.

An effective sensor fusion solution must not diminish the detection capability of the system when compared to each sensor evaluated independently, but also must meaningfully reduce the increased volume of nuisance alarms that accompany the addition of new sensors. The ideal

fusion scenario is the one which emphasizes each sensor's strengths while mitigating its weaknesses. Weakness, in this case, means either reporting a situation as an alarm when it is not, or not reporting an alarm when there is one. The current industry standard approach to sensor fusion is to use logical inference in a rule engine. The net effect of logical inference is to simply perform a logical AND on the outputs of two or more sensors, in effect combining multiple sensors into one. Intuitively we can understand that combining sensors this way combines their weaknesses as well as their strengths. This approach to sensor fusion actually provides an advantage to the adversary: where previously he needed to defeat multiple sensors, now he only needs to defeat the weakest sensor to compromise the perimeter. The test results presented bear this out: NAR and UAR are meaningfully reduced, but unfortunately so is the detection performance. This fails to create truly synergistic sensor fusion, and clearly we can do better.

The results show that logical inference is too simple, and may produce a system with a lower P_D than a system without fusion, whereas the machine learning approach can produce a system with a comparable P_D to a system without fusion, yet eliminates many of the nuisance alarms to which such a system is usually susceptible. Not only was the machine learning algorithm able to capture nearly all attempts of a sophisticated adversary to subvert detection by the system through exploiting known weaknesses, it reduced the combined NAR/UAR to barely measureable levels. Indeed, examination of the two nuisance alarms experienced by the system over 3 months of passive testing show they were caused by rabbits loitering in the maintenance access in a way that matches the signature of a crawling adversary using stealth to bypass both the seismic sensors and VMD. Machine learning is able to succeed decisively where the industry standard rule-based approach fails, because it employs advanced data analysis techniques to extract patterns of correlation between sensors. This allows them to report as if they were independent when their probability of detection is known to be strong, but combines them with others when their probability is known to be weak. This allows machine learning to avoid the pitfall of combining sensor weaknesses that limits the effectiveness of logical inference. Indeed, significant gaps in sensor performance that occurred during testing demonstrate that machine learning is able to draw accurate decision boundaries between real and nuisance alarms even in the face of inconsistent data that would foil rule-based approaches to sensor fusion. A key to enabling such performance is sensor technology which provides detailed data to properly inform decision-making algorithms. Currently, few vendors are willing to provide such data to the user in a straight-forward fashion, but as the security industry moves to demanding higher performance, the best systems will incorporate only those sensors capable of doing so.

The promising results motivate the continued work in this line of research. It would be worthwhile to continue this work by evaluating additional sensor types, perhaps focusing on sensors that will provide additional detection against threats of bridging over a barrier, or tunneling underneath, and enhancing the fusion algorithms to minimize the NAR from those sensors. Enabling the system and sensors to run the machine learning algorithms live should also be a focus, and performing sensor characterization and system bypass testing on the live system, verifying the results found in this study by post-processing the sensor data through the algorithms. Furthermore, it is hypothesized that the effectiveness of the machine learning approach in reducing the NAR will alter the conventional tradeoff between detection sensitivity and NAR, allowing sensors to be tuned to higher levels of sensitivity, improving complex decision-making capability, and increasing detection performance. Additional testing should

evaluate that hypothesis, in addition to incorporating nighttime and winter test conditions to allow a more thorough evaluation of the NAR-reduction capabilities of the machine learning process.

7 References

1. Ruben Martinez, Modified Normandy Barrier – A Passive Vehicle Barrier, SAND2012-6197P. Sandia National Laboratories, Albuquerque, NM, 2012.
2. Standard Test Method for Vehicle Crash Testing of Perimeter Barriers, ASTM F2656-07. ASTM International, West Conshohocken, PA, 2007.
3. Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems, 2nd Edition.* New York: Butterworth-Heinemann, 2007.
4. Jason Krein, *Rapid Extended Defense System – Enhancing Security,* SAND2011-6256P. Sandia National Laboratories, Albuquerque, NM, 2011.
5. Matthew J. Wingle, *Qualification Test and Evaluation of the Deitech Photon Advanced Active Infrared (AIR) Intrusion Detection System,* Sandia National Laboratories, Albuquerque, NM, March 2009.
6. Command and Control Display Equipment (CCDE) Information Interchange using XML, SEIWG-ICD-0101B. SEIWG. Available online: http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html.
7. James R. Cooke, Mark T. Lee, and John. P. Vanderbeck, *Binomial reliability table (lower confidence limits for the binomial distribution).* US Naval Ordnance Test Station, California, 1964.
8. Astronomical Applications Department of the U.S. Naval Observatory – Data Services, Table of Sunrise and Sunset Times, http://aa.usno.navy.mil/data/docs/RS_OneYear.php.

Appendix A

A.1 TESTING DATA

A.1.1 VMD Sensor

Table A-1 contains the results for the run tests comparing monochrome and color mode performance on the VMD sensor. The raw times for the tests are contained in the table.

Table A-1: VMD Results for Run Tests in Monochrome versus Color Mode

Trial	Mode	Approach	Distance (ft)	Path	Speed (ft/s)	Contrast	Total Test Duration (s)	VMD Detection	Time until Detection (s)	VMD Confi-dence Level	Response Time (s)
1	Monochrome	Run	81	4	15.8	L	5.12	Y	6		0.88
2				4	15.0	L	5.39	Y	5.39	19%	0
3				4	14.6	L	5.53	Y	7.36	42%	1.83
4				4	15.9	L	5.09	Y	5.09	43.3%	0
5				3	15.9	L	5.11	Y	5.11	42%	0
6				3	14.2	L	5.69	Y	6	11%	0.31
7				3	15.4	L	5.26	Y	5.26	36%	0
8				2	14.8	L	5.48	Y	5.48	18%	0
9				2	13.9	L	5.84	Y	5.12	28%	-0.72
10				2	15.5	L	5.24	Y	5.24	33%	0
1	Color	Run	81	4	18.2	L	4.46	Y	4.46	23%	0
2				4	16.4	L	4.95	Y	4.95	16%	0
3				4	15.9	L	5.08	Y	4.25	22%	-0.83
4				4	16.7	L	4.85	Y	4.85		0
5				3	13.2	L	6.13	Y	7.13	36%	1
6				3	16.7	L	4.86	Y	5.86		1
7				3	16.0	L	5.07	Y	7.82	22%	2.75
8				2	10.6	L	7.65	Y	8.65	40%	1
9				2	14.4	L	5.63	Y	5.63	16%	0
10				2	14.6	L	5.54	Y	7	52%	1.46

Table A-2 contains the results for the vehicle tests comparing monochrome and color mode performance on the VMD sensor. The raw times for the tests are contained in the table.

Table A-2: VMD Results for Vehicle Tests in Monochrome versus Color Mode

Trial	Mode	Approach	Distance (ft)	Path	Avg Velocity (MPH)	Detection	Total Test Duration (s)	Time until Detection (s)	Response Time (s)
1	Color	Polaris	48	1	9	N	----	----	
2					8	N	----	----	----
3					9	N	----	----	----
4					9.5	N	----	----	----
5					11	N	----	----	----
1	Monochrome	Polaris	48	1	7.5	Y	8	7.5	-0.5
2					9	N	8.7	0	----
3					9	N	7	0	----
4					10	Y	6.5	6.5	0
5					8	Y	6.4	7	0.6

A.2 NUISANCE DATA

All nuisance and unknown alarm rates are with respect to the raw number of alarms that occurred for the tables that follow.

A.2.1 Nuisance Summary

Table A-3 tabulates the raw nuisance alarms triggered by all the sensors.

Table A-3: Summary of Raw Nuisance Sources and Alarm Rates for All Sensors

Nuisance Summary	Photon	MicroPoint	REDS Footstep	REDS Vehicle	VMD	Total	Grand Total
Daytime Raw Alarms	6	66	180	450	24	**726**	**971**
Nighttime Raw Alarms	6	116	31	92	----	**245**	
NAR	0.12	1.10	0.30	0.93	0.36[1]	**2.37[2]**	**9.83**
UAR	0	0.74	2.45	6.14	0.09[1]	**7.46[2]**	

Note 1: Alarm rates do not include nighttime periods in alarm rate calculation

Note 2: While the REDS system was only active for 76.7 days and the VMD system for 53.7 days, the Total alarm rates for the collective system were calculated over the entire 98.8 day test period to better represent total performance.

A.2.1 Alarm Filter Explanation

Figure A-1 shows an example alarm sequence of sensor X for the same alarm source on the same day at the noted times. The alarm event occurs at 2:36:45 PM and the next at 2:36:50 PM which is a time difference of five seconds. According to the rule we developed since this is less than or equal to 30 seconds this second alarm is filtered and not counted. Likewise the third alarm happens nine seconds after the second alarm which by the same logic is filtered. Thus, this example series of three total alarms is filtered to only one alarm.

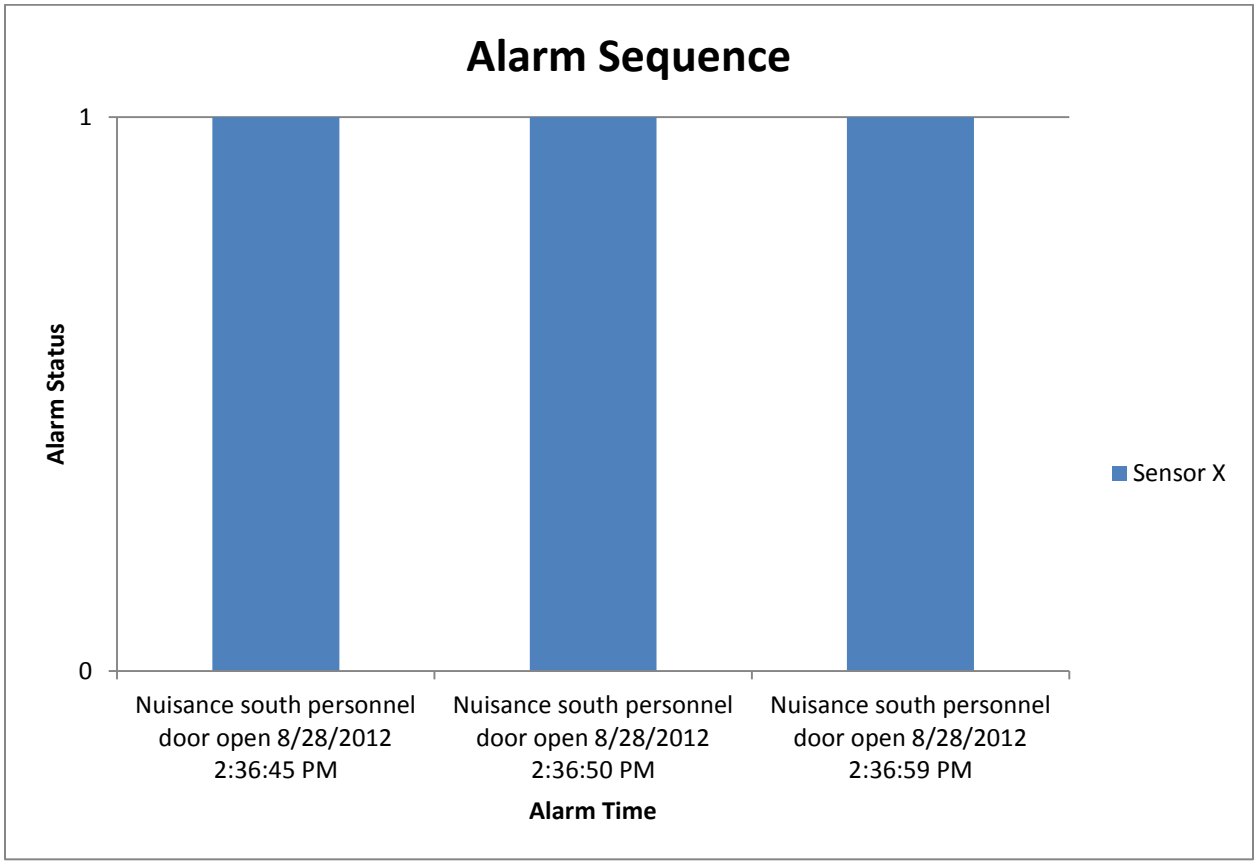


Figure A-1: Alarm Filter Applied to the Example Alarm Sequence for Sensor X

It is noted that this filter rule was implemented because the same alarm stimulus (e.g., rabbit tripping Photon IR beams) causing multiple alarms would most likely be counted as one event in a real installation. The operator can see that the alarm has tripped multiple times from the same source. Moreover, the operator would not secure the alarm on the AC&D system until the rabbit or nuisance source was cleared from the area by response or maintenance personnel. The 30 second rule to separate events as unique was chosen arbitrarily. There is no standard for the number of seconds between alarm events that considers those events unique. The raw number of alarms is presented in the tables below.

All individual sensor results are presented in the tables below.

A.2.2 Photon

Table A-4: Raw Photon Nuisance Sources and Alarm Rate

Alarm Source	Raw Alarms	Filtered Alarms	Raw NAR	Raw UAR
Daytime				
Rabbit	6	5	0.06	----
sub total	6	5	0.06	0
Nighttime				
Rabbit	1	1	0.01	----
Sunset	4	4	0.04	----
Poor Camera Visibility	1	1	0.01	----
sub total	6	6	0.06	0
Total	12	11	0.12	0

A.2.3 MicroPoint

Table A-5: Raw MicroPoint Nuisance Sources and Alarm Rate

Alarm Source	Raw Alarms	Filtered Alarms	Raw NAR	Raw UAR
Daytime			0.88	----
Sign on fence	87	64	0.02	----
Poor Camera[1] Visibility	2	2	----	0.54
Unknown	53	48	0.11	----
High Winds	11	11	0.88	----
sub total	153	125	1.01	0.54
Nighttime				
Sign on fence	449	319	4.55	----
Unknown	20	19	----	0.20
Rain	36	30	0.36	----
Poor Camera Visibility	60	55	0.61	----
sub total	565	423	5.52	0.20
Total	718	548	6.53	0.74

Note 1: Refers to camera blooming during sunset condition

Table A-6: Raw MicroPoint Nuisance Sources and Alarm Rates with Sign on Fence Event Excluded

Alarm Source	Raw Alarms	Filtered Alarms	Raw NAR	Raw UAR
Daytime				
Poor Camera[1] Visibility	2	2	0.02	----
Unknown	53	48	----	0.54
High Winds	11	11	0.11	----
sub total	66	61	0.13	0.54
Nighttime				
Unknown	20	19	----	0.20
Rain	36	30	0.36	----
Poor Camera Visibility	60	55	0.61	----
sub total	116	104	0.97	0.20
Total	182	165	1.10	0.74

Note 1: Refers to camera blooming during sunset condition

A.2.4 REDS

Table A-7: Raw REDS Footstep Nuisance Sources and Alarm Rate

Alarm Source	Raw Alarms	Filtered Alarms	Raw NAR	Raw UAR
Daytime				
Unknown	180	125	----	2.35
sub total	180	125	0	2.35
Nighttime				
Unknown	8	7	----	0.10
Rain	16	8	0.21	----
Poor Camera Visibility	7	7	0.09	----
sub total	31	22	0.30	0.10
Total	211	147	0.30	2.45

Table A-8: Raw REDS Vehicle Nuisance Sources and Alarm Rate

Alarm Source	Raw Alarms	Filtered Alarms	Raw NAR	Raw UAR
Daytime				
Unknown	442	432	----	5.76
Poor Camera[1] Visibility	8	8	0.10	----
sub total	450	440	0.10	5.76
Nighttime				
Unknown	29	29	----	0.38
Rain	8	8	0.10	----
Poor Camera Visibility	54	53	0.70	----
Rabbit	1	1	0.01	----
sub total	92	91	0.82	0.38
Total	542	531	0.93	6.14

Note 1: Refers to camera blooming during sunset condition

A.2.5 VMD

Table A-9: Raw VMD Nuisance Sources and Alarm Rate

Alarm Source	Raw Alarms	Filtered Alarms	Raw NAR	Raw UAR
Daytime				
Bird	1	1	0.02	----
Unknown	5	5	----	0.09
Rabbit	18	15	0.34	----
Total	24	21	0.36	0.09
Nighttime				
Rain	1	1	----	----
Poor Camera Visibility	16	16	----	----
Unknown	5	5	----	----

Distribution:

External Distribution:

James O. McLaughlin, jim@stonewatercontrols.com (electronic copy)
Stonewater Software Controls, Inc.
805 McCombs Avenue
Kannapolis, NC 28083

R. Allen Nolte, allennolte@msn.com (electronic copy)
Kontek Industries, Inc.
805 McCombs Avenue
Kannapolis, NC 28083

Kim Pocock, kpocock@kontekindustries.com (electronic copy)
Kontek Industries, Inc.
805 McCombs Avenue
Kannapolis, NC 28083

Barclay J. Tullis, barc@novelthink.com (electronic copy)
Novelthink
1795 Guinda Street
Palo Alto, CA 94303

Internal Distribution:

MS 1125	Jason J. Andersen	6532 (electronic copy)
MS 1361	Anthony R. Aragon	6833 (electronic copy)
MS 1361	Robert B. Berry	6833 (electronic copy)
MS 1010	Jeffrey G. Dabling	6533 (electronic copy)
MS 1125	Jake Deuel	6532 (electronic copy)
MS 1361	Ruth A. Duggan	6833 (electronic copy)
MS 1361	Calvin D. Jaeger	6833 (electronic copy)
MS 1361	Pamela Kissock	6833 (electronic copy)
MS 1125	Thomas K. Mack	6532 (electronic copy)
MS 0783	Ruben Martinez	6634 (electronic copy)
MS 0783	Chad W. Monthan	6634 (electronic copy)
MS 1361	Riyaz M. Natha	6833 (electronic copy)
MS 1361	Stephen Ortiz	6833 (electronic copy)
MS 0781	Jason Pelowitz	6523 (electronic copy)
MS 0136	J. Anthony Romero	0215 (electronic copy)
MS 1361	Carol Scharmer	6833 (electronic copy)
MS 1361	Mark K. Snell	6833 (electronic copy)
MS 0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories