SAND2012-6183C

Design and Performance Testing of an Integrated Detection and Assessment Perimeter System

Jeffrey G. Dabling
Sandia National Laboratories
Intelligent Systems & Controls
Albuquerque, NM 87185-1010
Email: jgdabli@sandia.gov

James O. McLaughlin
Stonewater Control Systems, Inc.
A Subsidiary of Kontek Industries
Evanston, Il 60201
Email: jim@stonewatercontrols.com

Jason J. Andersen
Sandia National Laboratories
Robotic and Security Systems
Albuquerque, NM 87185-1125
Email: jjander@sandia.gov

***Abstract*—Kontek Industries (Kannnapolis, NC) and their subsidiary, Stonewater Control Systems (Evanston, Il), have entered into a cooperative research and development agreement with Sandia National Laboratories (Albuquerque, NM) to jointly develop and evaluate an integrated perimeter security solution, one that couples access delay with detection and assessment. This novel perimeter solution is designed to be sufficiently flexible for implementation at a wide range of facility types from high security military installations to commercial power plants to industrial facilities of various kinds. A prototype section of barrier has been produced and installed at the Sandia Exterior Intrusion Sensor Lab in Albuquerque, NM. The prototype was implemented with a robust vehicle barrier 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. In this implementation, infrared sensors and fence vibration sensors are coupled with a video motion detection solution and a ground sensor solution. 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 Nuisance Alarm Rate and False Alarm Rate.**

***Index Terms*—perimeter security, sensor fusion, detection, assessment, VMD, NAR, performance testing**

I. Introduction

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 looking at how to increase standoff against specific threats beyond their current PIDAS, or to 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 nevertheless investigating the need to incorporate increased detection capability at their existing perimeter. Additionally, some new facilities coming online may have need for a perimeter security system that in one integrated system, can provide detection, threat assessment, and delay, without requiring the intensive ground disturbance or protracted delays required by traditional PIDAS installation.

It is unlikely that a single-line perimeter can attain the high probability of detection (P_d) and low nuisance alarm rate (NAR) of a full PIDAS, which has the benefit of an animal control fence with an engineered clear zone. However, in many applications, an extended perimeter outside of an existing PIDAS, or an upgraded perimeter for a low- to medium-security installation, does not have the high-level performance requirements that would justify that expense of 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 various facility requirements, and sufficiently configurable to provide higher performance in some installations, or permit trade-offs to reduce cost or increase ease of installation in other facilities.

In this environment, Kontek Industries (Kannapolis, NC) and their subsidiary, Stonewater Control Systems (Evanston, Il), have entered into a cooperative research and development agreement (CRADA) with Sandia National Laboratories (Albuquerque, NM) to jointly develop and evaluate an integrated perimeter security solution, one that couples access delay with detection and assessment. This novel perimeter solution is designed to be sufficiently flexible for implementation at a wide range of facility types, from high security military installations to commercial power plants to industrial facilities of various kinds. The underlying integration technology, derived from Stonewaters 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^{TM} system, shown in Figure 1, was the initial outcome of this collaboration. A prototype section has been produced and installed at the Sandia Exterior Sensor Testing Facility in Albuquerque, NM. The prototype system was implemented with a robust Sandia designed M50-rated 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, infrared sensors and fence vibration sensors are coupled with a video motion detection solution and a Sandia-designed ground sensor solution. The ability of the system to properly detect pedestrian or vehicle attempts to bypass, breach, or otherwise defeat the system will be

Fig. 1. ReKon™ Systems prototype installation

Fig. 2. Section of Modified Normandy Barrier (MNB)

characterized, as well as the Nuisance Alarm Rate and False Alarm Rate.

II. Design Overview

The goal is to develop a highly capable system that can provide effective detection and assessment integrated with a barrier, for use outside an existing perimeter, or to provide a detection perimeter where none exists. Such a system will likely not achieve the probability of detection (P_d) of a full PIDAS with an engineered clear zone and animal-control fence, but it is not intended to be a complete replacement for a PIDAS. Not all applications need the full P_d of a PIDAS, or cannot afford the price tag. Thus, one of the long-term goals of the project is to develop a system that can be installed for less than the cost of a full PIDAS. The primary performance goals for the prototype system include: M50 vehicle barrier rating, 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 technology that best fulfill those needs. The ReKon™ system was designed as an enhanced integration system. It was to be sufficiently flexible to allow the technology to integrate any available sensor, whether that sensor outputs an XML rich dataset, analog voltage, or a simple binary output. It was also designed to be sufficiently flexible to allow installation on various types of vehicle barriers, although some modification to the barrier, or addition of hardware, might be necessary to accommodate the cabling. 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 necessary. To that end, a field distribution box was mounted directly to the barrier, and two towers were integrated into the barrier design to not need separate installation. The towers and FDB can be seen in Figure 1. Although the towers were not utilized in the performance testing discussed in this paper, they offer the capability of mounting additional cameras, illumination systems, or additional equipment as desired.

A. Barrier

The barrier chosen for the prototype was the Modified Normandy Barrier (MNB) [1], designed by Sandia National Laboratories, shown in Figure 2. While the types of sensors chosen and the various mounting features may necessarily change depending on the barrier used, the intent of the ReKon™ System is to be somewhat barrier agnostic. Thus, this barrier has been used for the prototype, but it is not meant to indicate that only the MNB can be used with this system.

The MNB was chosen due to the ability to install it with minimal digging, high vehicle crash test rating (ASTM M50/P1) [2], and current popularity with many customers due to the difficulty to an adversary of hiding behind the barrier (the ability of the protective force to shoot through the barrier).

It has been crash-tested at Texas Transportation Institute (TTI), and achieved an M50/P1 rating with in-ground bollard supports installed every 40. Configurations of the barrier can be installed with fewer supports, but a lower crash rating is likely. Additionally, characterization of the barrier against both mechanical and explosive breaching has previously been conducted. [1]

B. Detection & Assessment

The test section included various complementary sensors to better evaluate the capability of the system to integrate multiple types of inputs. A diagram demonstrating how the sensors were arranged on and around the barrier is shown in Figure 3.

LightLOC Express from Woven Electronics (Simpsonville, SC) is a fiber optic break sensor that alarms when the light transmission loss through the fiber is greater than the set

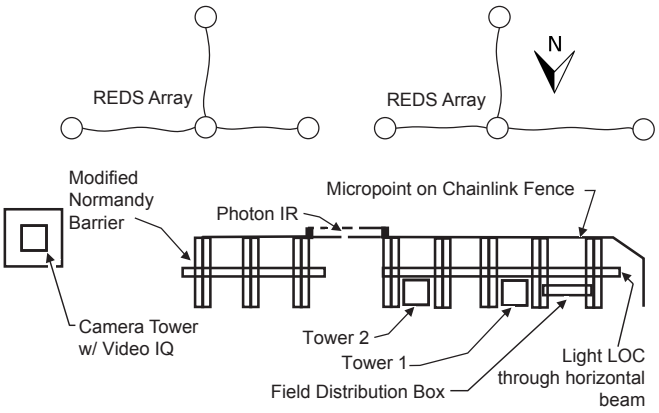

Fig. 3. Diagram showing sensor layout in prototype system

threshold. Essentially, it alarms when the fiber is broken, or when severely deformed. LightLOC was incorporated to show basic sensing capability for a possible barrier failure, either due to vehicle impact or breaching attacks. The cable was routed through a fixed conduit mounted on the secure side of the barrier, to hold it securely against the barrier, to better transmit any barrier deformation to the fiber. Due to the necessity of cauting a large transmission loss in the fiber prior to alarm, LightLOC is generally viewed as a low nuisance alarm rate (NAR) sensor, and provides the primary detection against vehicle threats.

The Intrepid MicroPoint II sensor from Southwest Microwave (Tempe, AZ) is a fence movement sensor. 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. The barrier was configured with a pedestrian 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 from Deitech (Torino, Italy), was installed across this pedestrian access. Both sensors serve to provide detection against pedestrian attempts to climb over or under the vehicle barrier, or unauthorized access through the pedestrian pathway, and thus MicroPoint and Photon IR are mounted effectively in series, each protecting a different portion of perimeter (fenced vs pedestrian access), and cannot be considered complimentary. To provide complementary detection against pedestrian and vehicle threats, additional sensors are mounted off the barrier. A video motion detection (VMD) system, the iCVR HD color dome camera from Video IQ (Bedford, MA), was mounted on a camera tower east of the barrier to enable full view of the entire test section and surrounding area. A seismic ground sensor solution, Rapid Extended Defense System (REDS) [3], developed by Sandia National Laboratories, was installed in the ground on the unprotected (south) side of the barrier.

C. Software

The system software architecture mirrors the physical barriers use of modularity to adapt to diverse installation environments. Like the barrier, the system software must be able to accept specialized sensor suites and fusion rules to match site conditions, and also must be able to accommodate customer specific security policies and legacy system integration requirements. A major functional requirement of the system was to provide a convenient, unified platform to integrate, monitor and manage disparate commercial off-the-shelf (COTS) sensors. A significant problem with adding COTS sensors to a system is that each additional sensor increases the volume of nuisance and false alarms in the system. To address this problem, the software provides a plugin framework to support implementing and evaluating different methods of sensor fusion to reduce NAR/FAR. Just as there is no one size fits all solution to integrated perimeter defense, the choice of algorithms to reduce NAR/FAR will also need to be adjusted based on the compliment of sensors chosen, threat analysis, and environmental conditions. A final high level functional requirement was to supply interfaces and adapters for integrating with existing legacy or modern command and control infrastructures. Four high level design criteria guided our architectural choices: *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 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 provided system-to-system level integration, external APIs and message formats were implemented based on the Department of Defense (DoD) Security Equipment Integration Working Group (SEIWG) Interface Control Document for Command and Control Display Equipment (CCDE) Information Interchange using XML (ICD-0101B). SEIWG is a multi-service collaboration within the 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, as well as 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.

To address security requirements, the system supports declarative, message level security policies via WS-Security. Where SSL/TLS apply security policies to end-to-end transport in a way that is non-declarative (i.e. programmatic), WS-Security can apply security policies to individual messages through the use of policy files. In a large, distributed system such as a perimeter security system, messages are expected to relay through multiple transport endpoints and be received by consumers at multiple destinations. If the system only employed SSL/TLS, then the message would lose any security guarantees beyond the first first endpoint. Only by applying policy to the message itself can security guarantees be maintained in a distributed system like ours where the message may end up at multiple destinations. Employing declarative security policies also allows changes to those policies to be non-invasive, e.g. no code needs to change in the application to support changes in policy. Our system enforces security policies on all messages coming in and out of the application through global policy enforcement points. All messages must travel through these enforcement points and will be rejected unless there is a policy authorizing it. Declarative policies provide the customer flexibility to decide what type of encryption and authentication the system will require.

D. Modular Software Design

To provide modularity, the system software is built around a Message Bus construct. The Message Bus provides a single point of entry and egress for all messages entering and leaving the system. This provides a convenient checkpoint for security policy enforcement. Next content-based routing rules are applied to the message to assign it a topic and publish it. Services subscribe to topics on the Message Bus to receive the messages they are interested in. Any response returned by the service goes back to the Message Bus where it can be intercepted and published for additional processing by other services. 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 an existing topic, or a new message is published to existing services. 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.

E. Software System Capabilities

Adapters harvest sensor input over a variety of communication media: RS-232/485, UDP, TCP, and 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, JMS, TCP, and UDP. Security is enforced via WS-Security policies. 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 the nature of those changes 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 Video IQ 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.

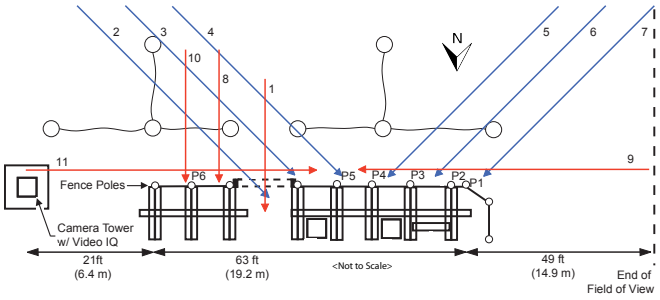

Fig. 4. Diagram of Test Paths

III. Performance Testing

Performance testing was split into two categories: individual sensor performance and system level performance. Individual sensor performance was necessary to characterize each sensor's strengths and weaknesses in addition to verifying satisfactory performance against adversaries. The threat was defined to be a walking, running, belly-crawling, or bear-crawling intruder with the capability to approach with a vehicle. Additionally, groups of three to four adversaries were considered. During performance testing, test path distances and intruder speeds were recorded along with timing information. Approximate speeds for intruder approaches (unless noted otherwise) were 4 ft/s (1.2 m/s) for walking, 14 ft/s (4.3 m/s) for running, 1 ft/s (0.3 m/s) for both crawling methods, and vehicle speeds varied.

A. Test Methodologies

Figure 4 shows the different test paths considered during sensor characterization and system testing. Each test path is numbered and referenced in the sections below.

1) Individual Sensor Characterization: Each sensor was individually characterized with the exception of REDS and LightLOC. LightLOC is a simple switch type sensor thus the only testing conducted was to simulate a break in the fiber or to bend the fiber. REDS data was collected during the characterization of the other sensors. The tests conducted for each sensor are described below.

- Photon
  The following tests were conducted for the Photon sensor:
  - Walking (path 1)
  - Running (path 1)
  - Belly crawling (path 1)
  - Bear crawling (path 1)
- Intrepid MicroPoint II
  The following tests were conducted for the MicroPoint sensor:
  - Climbing on fence poles (paths P1 - P6)
  - Climbing on fence fabric between poles (paths P1 - P6)
  - Cutting on fence fabric between poles (paths P1 - P6)

There were a total of 6 poles that were tested when climbing as referenced in Figure 4. When conducting the fabric climb tests, the test subjects climbed in between poles 1-6 and an additional fabric panel that was adjacent to pole 1 for a total of eight fabric sections. In addition to the above tests, five fabric lift tests were conducted to verify that this was not a feasible bypass method.

- REDS
  The following tests were recorded for the REDS sensor:
  - Running (paths 1, 11, 9)
  - Belly crawling (paths 1, 9)
  - Bear crawling (paths 1, 9)
  - Polaris Ranger ATV 4x4 (path 1)
  - Dodge Minivan (path 1)
- VideoIQ
  Testing for the VideoIQ system was conducted both in color mode and in monochrome mode, always in the daytime. No testing was performed at night due to illuminator malfunction and project schedule. The following tests were conducted in color mode:
  - Walking (paths 1 - 7, 9, 11)
  - Running (paths 1 - 7, 9, 11)
  - Belly crawling (paths 1, 9)
  - Bear crawling (paths 1, 9)
  - Polaris Ranger ATV 4x4 (path 1)
  - Dodge Minivan (path 1)

  The following tests were conducted for the VideoIQ system in monochrome mode:
  - Running (paths 5 - 7)
  - Polaris Ranger ATV 4x4 (path 1)
  - Dodge Minivan (path 1)

2) System Level Performance: After characterizing each sensor against simple adversary behaviors, more complex methods were explored to attempt to bypass the entire system of sensors. There are only five fundamental ways to bypass the barrier: climb over the fence, cut through the fence, bridge over the barrier, tunnel under the barrier, and drive a vehicle through the barrier. The latter was not tested during this effort. The system level testing is different from the individual sensor characterization in that every system test included one of the scenarios mentioned above. The following tests were conducted for the system:

- Bridging Attempts
  - Three walking and bear crawling subjects cloaked with tarp with ladder (path 1)
  - Three walking subjects shoulder to shoulder with ladder (path 1)
  - Three walking subjects cloaked with styrofoam door shoulder to shoulder with ladder (path 1)
  - Bear crawling subject dragging a ladder (path 1)
  - Drive golf cart to barrier then subject gets on roof to jump over barrier (paths 1 and 9)
  - Drive Ford F-350 truck to barrier then subject gets on roof to jump over barrier (paths 1 and 9)

TABLE I
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 II
SOUTHWEST 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

- Tunneling Attempts
  - Three walking subjects cloaked with rigid tarp (8 ft. x 10 ft.) digging with shovel (path 1)
  - Three bear crawling subjects cloaked with tarp digging with hand trowel (path 1)
  - Three walking subjects in group digging with hand trowels (path 1)
  - Bear crawling subject digging with hand trowel (paths 1 and 8)
- Climbing Attempts
  - Walking subject climb the fence (paths P1 - P8)
- Cutting Attempts
  - Walking subject cloaked with styrofoam door cut through fence between poles (paths P1 - P8)
  - Walking subject with backpack cut through fence between poles (paths P1 - P8)

B. Stand-alone Sensor Performance

Table I summarizes the Photon sensor test results. The Photon sensor was tuned to ensure an adversary could not crawl under the bottom beam and that a running adversary could not run through faster than the phasing of the beams. Table II summarizes the MicroPoint sensor test results. The climb tests consisted of climbing to the top of the eight foot fence and holding position at top for a couple of seconds. The cut tests consisted of performing no more than eight cuts forming an opening at the bottom of the fence fabric. Table III summarizes the REDS sensor test results. Detections on REDS were defined as either the vehicle or human footsteps rule triggering during the test attempts. REDS was off-line when walking data was collected for other sensors and thus is not reflected in the table.

TABLE III
REDS TEST RESULTS

Approach	Distance Traveled (ft)	Path	Speed (ft/s)	Detections/ Repetitions	P_d @ 95% Conf.
Run	48	1	14	17 / 30	?
Run	125	11	19	28 / 30	80
Run	125	9	18	10 / 10	74
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

C. Sensor Fusion Performance

Two approaches to sensor fusion were evaluated. The first approach fused logic states output by the individual sensors by considering coincident events over a time window. The second approach applied statistical machine learning techniques to more detailed assessment data extracted from the sensors after the fact (except for Video IQ, 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. Due to some equipment malfunction there was not always a full compliment of sensor data for all the alarm events under consideration. The experiment evaluated the results of combining REDS acoustic alarms and VideoIQ VMD alarms with Photon IR and Southwest Micropoint alarms to eliminate nuisance alarms from Photon IR and Southwest Micropoint.

The dataset for both tests contained 906 total alarm events recorded from both Southwest Micropoint and Photon IR. The 906 events were manually sorted into 640 real alarms and 266 nuisance alarms. The following statistics were gathered to measure the effectiveness of each approach:

- *True Positives*: alarm is real and predicted as real.
- *False Positives*: alarm is nuisance and predicted as real.
- *False Negative*: alarm is real but predicted as nuisance
- *Precision*: % positive predictions that were correct

$$\frac{TruePositives}{TruePositives + FalsePositives}$$

- *Recall*: % real alarms caught

$$\frac{TruePositives}{TruePositives + FalseNegatives}$$

- *F1 Score*: harmonic mean of Precision and Recall
- *Nuisance Elimination*: % of nuisance alarms eliminated

The methodology for the logic state fusion experiment was to configure the Complex Event Processor to aggregate alarm events from VideoIQ or REDS that signify human or vehicle detected and correlate them separately with either Photon IR or Southwest Micropoint alarms over a 15 second window of time. The correlation events were then sent to the Rule Engine where a positive correlation would trigger the generation of

TABLE IV
VIDEOIQ TEST RESULTS

Mode	Approach	Dist. Traveled (ft.)	Path	Speed (ft./s.)	Contrast	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	74
	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	74
	Run	81	2, 3, 4	15	L	14 / 25	?
	Run	81	5, 6, 7	14	L	9 / 26	?
	Belly Crawl	18	1	1	M	4 / 30	?
	Belly Crawl	18	1	1	H	10 / 10	74
	Belly Crawl	71	9	1	M	3 / 8	?
	Bear Crawl	18	1	1	M	1 / 10	?
	Bear Crawl	18	1	1	H	10 / 10	74
	Bear Crawl	71	9	1	M	3 / 8	?
	Polaris Veh. Cont.	48	1	13	—	3 / 16	?
	Polaris Veh. Start/Stop	48	1	13	—	0 / 5	?
*	Run	81	5, 6, 7	15	L	10 / 10	74
Monochrome	Polaris Veh. Start/Stop	48	1	13	—	3 / 5	?
	Minivan Start/Stop	48	1	15	—	0 / 4	0
	Golf Cart Start/Stop	48	1	8	—	2 / 5	?
*	Run	81	5, 6, 7	15	L	10 / 10	74

an alarm event. The system was then set to run live against real data as it was generated by test intrusions and real environmental nuisances. The machine learning approach was evaluated offline because the more detailed sensor data it required was not available online, and also because of the need to acquire a dataset large enough to both train the system and evaluate its performance. Additionally, in order to assess the contribution of each sensor to the overall effectiveness of the machine learning classifier, a ceiling analysis was performed by generating separate datasets with different sensor combinations:

- *pir_w*: Photon IR with weather only
- *pir_wr*: Photon IR with REDS and weather
- *pir_wv*: Photon IR with VideoIQ weather
- *pir_wrv*: Photon IR with REDS, VideoIQ and weather
- *swm_w*: SW Micro and weather
- *swm_wr*: SW Micro with REDS and weather
- *swm_wv*: SW Micro with REDS and VideoIQ
- *swm_wrv*: SW Micro with REDS, VideoIQ, and weather
- *pir_swm*: Combined Dataset Photon, SW Micro, REDS, VideoIQ, and Weather

The dataset was randomized and split into 60% training data and 40% test evaluation data. For each dataset above, the machine learning algorithm was then trained on the training data and its prediction performance evaluated with the separate test dataset. Since the dataset was small and performance would vary based on which test cases did not have a corollary in the training data, each dataset was run through 200 training iterations, each time randomizing the data, retraining the classifier, and measuring its performance against the new test dataset. The mean of each statistic was calculated after the last iteration for each dataset.

TABLE V
SENSOR FUSION EVALUATION RESULTS

Dataset	T Pos	F Pos	F Neg	Prec	Recall	F1	NE
logic state	514	14	126	0.973	0.803	0.879	0.938
pir_w	185.555	4.740	2.755	0.975	0.985	0.980	0.297
pir_wr	185.495	3.475	2.835	0.982	0.985	0.983	0.495
pir_wv	186.730	1.965	1.240	0.990	0.993	0.991	0.733
pir_wrv	186.270	1.685	1.780	0.991	0.991	0.991	0.770
swm_w	65.365	0.870	2.340	0.987	0.966	0.976	0.991
swm_wr	64.915	1.620	2.325	0.976	0.966	0.970	0.984
swm_wv	66.315	0.365	1.115	0.995	0.983	0.989	0.996
swm_wrv	65.695	0.760	1.425	0.989	0.979	0.984	0.992
combined	253.785	1.855	1.505	0.993	0.994	0.993	0.983

IV. DISCUSSION

The evaluation results reveal obvious weaknesses in sensor fusion using only logic states, and significant promise in 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 is way more resilient in the face of sensor loss. The test data was also 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 under going maintenance and would have normally been placed into access mode. For the machine learning experiment, most if not all of 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. The 80% recall score posted by logic state fusion

indicates that it is not able to combine the sensors without combining their weaknesses as well, and overall results in a significantly weaker system than one that considers each sensor individually.

The machine learning ceiling analysis reveals that the largest contributors to nuisance elimination are the VideoIQ for Photon IR, and weather for Southwest Microwave. Largely this is because they 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 really provides only truth state values regarding detection, its contribution wasn't as effective as VideoIQ. Similarly, the combination of weather data with Southwest Microwave proved so effective, there was little room for REDS to make a contribution with the limited data it provides. VideoIQ did experience some trouble discerning subjects standing flush to the fence, and a number of false negatives occurred while Southwest Microwave was being tuned (e.g. in maintenance mode) and the subject would trigger an alarm without approaching the fence (he was already there). Without an approach to the fence neither REDS nor VideoIQ had a chance to identify the subject. Overall, machine learning displayed outstanding results with the ability to eliminate over 98% of nuisance alarms and maintain almost perfect recall for true alarms. Most if not all false negatives can be explained by sensor malfunction, situations with other alarms already present, or the system undergoing maintenance.

More sensors were included than might be implemented in some real world installations, due to the desire to evaluate the ability of the ReKon™ system to integrate multiple sensor phenomenologies and output types.

A. Sensor Characterization

The Photon and MicroPoint sensors provide line detection for the barrier. The issue associated with line sensors is that it is possible to bypass by bridging or tunneling the sensor. It is typical to compliment line sensors with a sensor that provides volumetric detection. The VideoIQ VMD and REDS sensors provide this complimentary coverage. However both VideoIQ and REDS have weaknesses. VideoIQ performed poorly in classifying with confidence both belly-crawling and bear-crawling adversaries when the contrast between the adversary and the background was not high. However, when the test subject stood up after the tests were complete and walked back to the start VideoIQ detected this. VideoIQ detected nine of the ten bear-crawl tests conducted on path 1 as the subject returned to the start of the test. Additionally, VideoIQ performed poorly against vehicles approaching the barrier tangentially. During the system testing it was observed that VideoIQ performed better when the vehicle traveled radially in or out of the field of view. REDS performed poorly detecting a bear-crawling adversary. We believe this is due to four points of contact with the ground and that it does not generate the same level of activity that walking, running, or belly-crawling do.

B. System Testing

The methodology used to select the bypass method for the barrier is as described in section III-A. The methods used to approach the barrier were based on the weaknesses of both VideoIQ and REDS sensors. The results highlight that it is possible to bypass either REDS or VideoIQ with the methods tested on the approach to the barrier. When the adversary reaches the barrier it will be necessary to either bridge or tunnel. REDS performed well against tunneling attempts when the soil content is not the same composition of sand. VideoIQ performed well at detecting the bridging attempts conducted during testing. It is clear that unless camouflaging is used during bridging this method is not feasible.

V. Conclusion

A perimeter defense system must be customizable to the unique conditions of each installation site in order to provide the most secure solution to the customer. To permit customization, the product must be modular and allow the solution to be assembled from the best selection of components. Similarly the software platform for integrating sensors must also be highly flexible and modular to expedite the process of bringing together the best sensors for a given threat environment as well as support integration into existing security technology infrastructure. However, deploying multiple sensor systems on the perimeter significantly increases the amount of false and nuisance alarms security personnel must respond to. The software platform must also provide a framework for plugging in different methods for fusing sensor data to reduce the false and nuisance alarms best suited to the installation environment. The ReKon™system has been designed to meet all these requirements.

A frequent criticism of sensor fusion as applied to physical security is that combining sensors together combines their weakness as well as their strengths. Often this produces conditions in which an adversary only needs to exploit vulnerabilities in one sensor in order to defeat the whole assembly. When this situation is true, it clearly produces a less capable detection system than when all sensor inputs are evaluated individually. Conversely, if each sensor is evaluated individually the overall volume of nuisance and false alarms increases by a multiple of the number of sensors in the system. The ideal fusion scenario is the one which exploits each sensor's strength but eliminates their weaknesses. Weaknesses in this case mean either reporting a situation as an alarm when it is not or not reporting an alarm when there is one. To avoid this, a sensor fusion algorithm needs to know under what conditions a sensor's performance is error prone, which requires a sensor to supply information such as probabilities and input values over a threshold. The test results show that logic state fusion is too simple, producing a system with lower probability of detection, but the machine learning approach produces a system with comparable probability of detection to a system with no fusion yet eliminates virtually all the nuisance alarms such a system is susceptible to.

A system has been demonstrated that can integrate various types of sensor inputs, which allows for incorporation of user-specified algorithms to further filter the data if desired. The suite of sensors chosen for this prototype demonstration is not intended to be a panacea, a solution for all possible installations. Sensor choices for a real installation need to be determined based on the unique requirements for that site.

ACKNOWLEDGMENT

The authors would like to acknowledge the vital work of Mariusz Stanisz and Paul Cappello with Stonewater Control Systems for the software design and integration that made this project possible. 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.

REFERENCES

[1] R. Martinez, *Modified Normandy Barrier - A Passive Vehicle Barrier*, SAND 2012-XXXX, Albuquerque, NM: Sandia National Laboratories.

[2] ASTM F 2656-07, *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*, West Conshohocken, PA: ASTM.

[3] J. Krein, *Rapid Extended Defense System - Enhancing Security*, SAND2011-6256P, Albuquerque, NM: Sandia National Laboratories.