# (U) Physical Security Against Explosive Threats: Standoff Magnetic and Electro-optical Sensing and Target Characterization

21 October, 2012

Gregory Schultz[1], Samuel Segal-Jensen[1], Jonathan Miller[1], Jack Foley[2]

[1]White River Technologies, Inc.[†]
3 School House Lane, Hanover, NH 03750 USA

[2]Sky Research, Inc
PO Box 267, Scituate, MA, 02066 USA

## ABSTRACT

Physical security threats associated with asymmetric warfare are emerging both domestically and throughout the world at an alarming rate and thus the need for effective person-borne improvised explosive threat detection is clear. Multi-modal sensor packages capable of detecting and classifying suicide bombers or other person-borne explosives can be effective at standoff distances that remove monitoring personnel from the danger zone. We describe the rapid development and deployment of a multi-sensor person-borne threat detection system that interrogates subjects under conditions ranging from structured entry control points where single individuals are scanned to unstructured crowds in which a large number of subjects are simultaneously in view and traversing an area of interest in arbitrary directions. Utilizing complementary characteristics of electro-optical recognition and magnetic interrogation (target detection, localization, and discrimination), we combine sensor data to enable improved detection and reduced false alarms over single modality systems. The modular system comprises a fully unattended and autonomous monitoring unit cued by pyrotechnical and other electro-optical sensors to invoke an array of magnetic field detectors. The array of highly sensitive atomic magnetometers detect disturbances in the Earth's field to indicate anomalous ferrous materials that may be associated with hazardous threats such as concealed weapons

[†] formerly of Sky Research, Inc., Hanover, NH

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **OCT 2012** | **N/A** | **-** |

4. TITLE AND SUBTITLE
**Physical Security Against Explosive Threats: Standoff Magnetic and Electro-optical Sensing and Target Characterization**

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
**White River Technologies, Inc. 3 School House Lane, Hanover, NH 03750 USA**

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**See also ADM202976. 2012 Joint Meeting of the Military Sensing Symposia (MSS) held in Washington, DC on October 22-25, 2012.**

14. ABSTRACT
**Physical security threats associated with asymmetric warfare are emerging both domestically and throughout the world at an alarming rate and thus the need for effective person-borne improvised explosive threat detection is clear. Multi-modal sensor packages capable of detecting and classifying suicide bombers or other person-borne explosives can be effective at standoff distances that remove monitoring personnel from the danger zone. We describe the rapid development and deployment of a multi-sensor person-borne threat detection system that interrogates subjects under conditions ranging from structured entry control points where single individuals are scanned to unstructured crowds in which a large number of subjects are simultaneously in view and traversing an area of interest in arbitrary directions. Utilizing complementary characteristics of electro-optical recognition and magnetic interrogation (target detection, localization, and discrimination), we combine sensor data to enable improved detection and reduced false alarms over single modality systems. The modular system comprises a fully unattended and autonomous monitoring unit cued by pyrotechnical and other electro-optical sensors to invoke an array of magnetic field detectors. The array of highly sensitive atomic magnetometers detect disturbances in the Earth's field to indicate anomalous ferrous materials that may be associated with hazardous threats such as concealed weapons**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **SAR** | **8** | |

We discuss the development and operations of the integrated systems including assessment of alternative magnetic sensing technologies and controlled source excitation for improved signal-to-noise ratios and advanced target characterization. In the structured crowd scenario our system can be configured within a layered security system with subjects pre-screened and under cued interrogation. In unstructured crowd scenarios, no such control is imposed and methods of reliable detection with low false alarms are desired even when subjects range between full optical visibility and full occlusion. The system is currently being used in-theater as a stand-alone checkpoint screening tool but can also be configured as a fully integrated security monitoring system encompassing multiple, networked ground station nodes inconspicuously deployed. Because improvised targets of interest have great variability in shape and material content, we rely on size and mass distribution features that are correlated with magnetic dipole moments.

Keywords: Magnetic Sensing, Magnetometers, Force Protection, Integrated Base Defense Systems, Military Sensing, Improvised Explosive Device

## 1.0 Introduction and Background

High casualty rates and associated disruptions to operations accentuate the need for enhanced protection of deployed forces. The Army has specifically identified urgent force protection needs at forward operating areas such as combat outposts (COPs), patrol bases (PBs), entry control points (ECPs), and traffic control points (TCPs). Current requirements emphasize defense against person-borne threats, namely person-borne improvised explosive devices (PBIEDS). Coupled with recent suicide bomb events in unstable regions of Southwest Asia and Africa, long-standing Urgent Operation Need Statements for ECPs and evolving requirements for Integrated Base Defense Security Systems (IBDSS) as well as emerging in-theatre requirements clearly define operational needs for improved physical security.

At many forward operating and special operations/low intensity conflict (SOLIC) areas, the US Department of Defense (DOD) (and increasingly the Department of State; DOS) are housing personnel in temporary facilities that may only provide limited security. Traditional physical security measures employed at fixed installations are not generally available during the installation of these less permanent facilities. Therefore, a critical physical security challenge is improving efficiency in the deployment of sensor modules in both tactical small-unit scenarios and in larger layered security systems (especially during drawdown or transition activities). Current systems require too much time to set-up, protect, sustain, and relocate (i.e., not "plug-and-play" ready); are not easily controlled from a single operating environment via fusion/automatic logic; and are not transitioned quickly enough to the warfighter.

**Figure 1. Left: Entry control point to a forward operating base. Middle: Typical Afghan National Army traffic control point. Right: Destruction and carnage at the scene of a suicide bombing attack in Damascus in May 2012 (Source: EPA/Syrian News Agency).**

# 2.0 System Description

The detection of concealed person-borne improvised explosive devices on individuals has been and remains a major concern of military personnel and law enforcement, and is especially challenging for US military operations in urban areas. Suicide bombers create weapons to maximize the casualties. Usually these weapons are comprised of explosives and shrapnel (metal screws, bolts, ball bearings). A PBIED detection capability is critically needed not only for operations during open hostilities but also during stability and support operations, as well as force protection operations as either an initial entry force or as a guarantor force to provide security for other forces.

Specialized unattended ground sensors comprised of "smart" magnetic detector arrays can detect weapons that produce magnetic signals above a certain threshold. We have developed a simple and robust multi-modal sensing system to detect PBIEDs and metal-infused explosives concealed under an individual's clothing. The SubtleMadness system combines remote unattended magnetic and electro-optical arrays camouflaged in natural (rocks or buried) or engineered (traffic cones, curbs) structures to detect hazardous materials associated with weapons and concealed explosives.

A combination of electro-optical and magnetic sensing techniques have marked advantages over other methods for ground-based intrusion detection systems. Specifically, passive magnetic monitoring has several operational advantages over active EM (e.g., metal detector or radar) and line-of-sight limited (e.g., camera, point source directed energy interrogation) techniques, including affordability, reliability, covertness, and an unobtrusive, all-terrain, all-weather, 360° view of avenues of approach for interdiction purposes. Suspect persons carrying concealed weapons or PBIEDs that are detected by covert magnetic systems do not know their actions are being recorded and analyzed, affording great advantage to protective forces.

Because magnetometry is a passive measurement, data can easily be acquired simultaneously from an array of distributed sensors and compiled by a data acquisition system. Commercial off-the-shelf (COTS) magnetic sensors have been ruggedized for land-based, airborne, and marine applications and can be readily integrated with an event detection processor and telemetry system. The ruggedness, availability, and high rate of productivity of COTS magnetometers, coupled with robust, reliable, and easy to use processing software were exploited to develop the current version of SubtleMadness. This system has been well-characterized and deemed suitable for operational use.

## 2.1. Sensor Components

SubtleMadness consists of a operator control station (OCS) that includes a power transmitter station, data acquisition and processing unit, touch screen display, and the remote unattended ground sensor (UGS) nodes. The power transmitting station provides power to all system components and provides all electrical interfaces between the UGS nodes and the OCS. Also integrated into the OCS, the processing and display unit runs the graphical user interface software displaying important system information including detection alarms and system status. The UGS nodes can be either self-powered (via internal


**Figure 2. Left-to-Right: The two primary system components: 1) remote sensor array concealed in traffic cones and 2) operator control station (OCS). Photo of OCS with power transmitter (foreground) remoted from sensors (background). Photo (top) and screen capture (bottom) of SubtleMadness display in single gate screening mode (two sensors) and trip wire mode (multiple sensor nodes). In the trip wire mode, the system displays the zone of the alarm as well signaling audible tone for the operator at the OCS location.**

battery) or remotely powered (via cable interconnect) and contains network multiplexing capability for numerous nodes. The UGS nodes are most commonly camouflaged in traffic cones to create a virtual "trip wire" to detect individuals with anomalous metallic materials.

A robust and versatile power supply enables the system to be powered by a wide range of alternating current (AC) or direct current (DC) sources as well as running from an internal battery during brown-out or black-out conditions. The current wireless link is capable of standoff operation at up to 1 kilometer (km) line-of-sight. Current forward operations do not utilize the wireless option, but instead make use of the sensor interconnect cable, which is capable of remoting the sensor nodes up to 500 meters from the interrogation area. When using a cabled data connection, standoff distance is limited only by the ability to create computer network style infrastructure. The system self-calibrates and performs built-in check and adaptive corrections to remove ambient noise.

## 2.2. Operational Concepts

The objective of the Entry Control Point (ECP) is to prevent unauthorized personnel or vehicle access while attempting to maximize traffic flow. An ECP guard force is a dedicated element with responsibility to control access to an operating area or base camp by conducting necessary searches and screening to prevent entry of unauthorized persons, vehicles, or cargo. The first priority of an ECP is to maintain perimeter security. The ECP must be designed to have security features that protect against vehicle-borne threats and illegal entry. An ECP should be designed for three key functions: 1) facilitate access control, 2) enhance the defense-in-depth concept, and 3) provide effective risk mitigation. The Access Control Zone is the main body of the ECP - it comprises guard facilities, vehicle and personnel inspection areas and traffic management equipment used by security forces.

Outer area screening sensors that are unattended and concealed in plain sight provide a first line of defense in the layered defense concept. Because there is no current technology that provides 100% probability of detection and 0% false alarm rate, the Army is pursuing a layered approach with increasing scrutiny and complexity in interrogation methods as suspects progress closer to the core operating area under protection.

SubtleMadness can be deployed quickly and efficiently and can be easily camouflaged, making it nearly transparent to inbound personnel. This type of technology affords security forces early warning and detection capability with sufficient standoff (>100m – via an interconnect cable or telemetry) to significantly reduce risk to personnel. The system provides visual and audible alarms that inform security forces (at the Guard tower or Command Post) of a potential threat while maximizing throughput during this initial screening. This real time screening eliminates a queue and thus a target of opportunity for the suicide bomber. Additional personnel are not required to man the system or interpret data. The individual

is either designated a green for "go" or red for "no go". On a detect event the audible alarm would sound and the targeted individual can then be segregated (clean lane / dirty lane) from other inbound personnel and further interrogated by other technology.

The operational concept for deployment of this system is quite simple. An array of two or more UGS sensor nodes are deployed and concealed (e.g., under traffic cones) for inconspicuous monitoring of a corridor or checkpoint area. Experimentation to-date has indicated that sensor separations of 2-10 meters are ideal for most scenarios to ensure good overlap between potential alarms. The area between each UGS node is designated as a zone that is inspected at a rate of 20 Hz. Data from each zone is filtered processed and analyzed for suspect anomalies. Preset thresholds, based on characterization of known contemporary targets, form the basis for the automatic target detection and alarm generation. When an alarm is determined, a graphical user interface provides both visual and audible cues to the operator. In addition, a source localization algorithm provides the location of the alarm within the zone indicated.

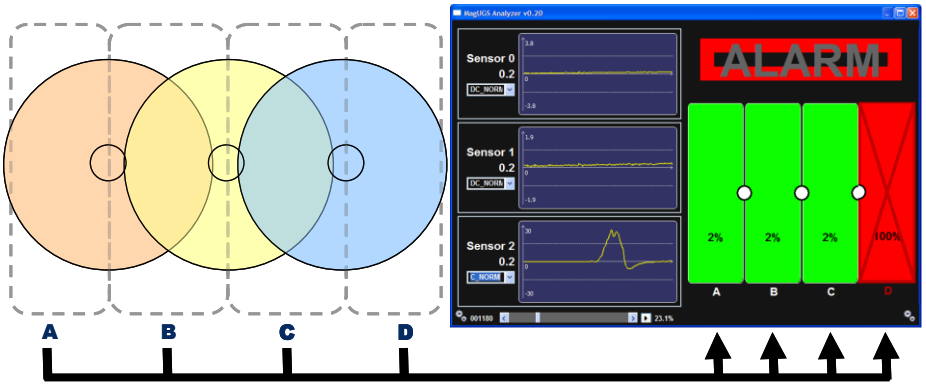


**Figure 3. The operational concept comprises and array of sensors that define zones through which subjects under investigation pass as they move. Each zone is investigated for suspect metallic materials; an alarm sounds and is displayed when the detection criteria have been met. An indicator also displays the location of the source of the alarm on a real-time graphical user interface display.**

## 3.0 System Testing

We conducted a preliminary capabilities demonstration of an early prototype version of the system at Camp Edwards in January 2009. For this demonstration, DOD established a simulated checkpoint station, through which multiple subjects advanced. Some of the subjects carried explosive simulants embedded with metal fragmentation. The identity of these target subjects was unknown to the system operators. The capabilities demonstration comprised a total of 10 trials each consisting of the 10 subjects advancing through the checkpoint (for 100 total realizations). Walkers advanced through a gateway defined by two sensor cones spaced approximately 3 meters apart. Upon entry, walkers turned around at a predetermined location and exited to the left side of the gate (see Figure 4). The order of the walkers was varied for each trial to ensure randomization.

Figure 4 shows an example of the primary sensor response for varying target types. These engineering test data were used to validate automated detection and classification algorithms. The initial step in the data analysis process involved applying signal processing techniques to transform the data into a suitable form based on a physical understanding of the underlying signal phenomenology (e.g., Schultz and Foley, 2008). A pre-screener was developed to quickly declare whether the suspect anomaly under investigation exhibits features consistent with concealed explosives. Fusion techniques combining the output of individual sensors (magnetic and infrared electro-optical) were investigated to reduce the influence of noise and clutter. Previously collected data were used in algorithm development and served to help address algorithm robustness and statistical significance. Simulated data were also used to augment this process and provided an additional level of confidence by enabling comparison against a number of field-proven systems.

Major components of the signal processing used algorithms from previously-developed munitions detection software. Data preprocessing consists of despiking, DC offset and detrending, layered filtering

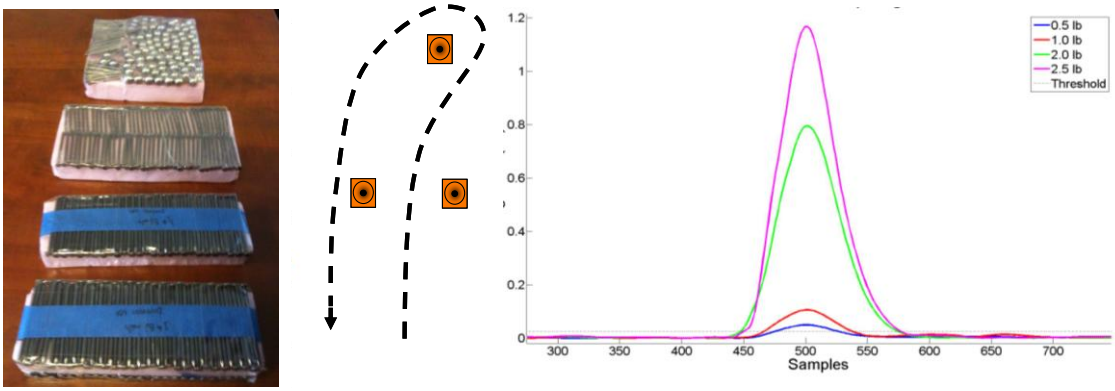


**Figure 4. Example test simulants and sensor target responses for varying target types.**

and smoothing, and Hilbert transform. The Hilbert transform step (Blakely, 1996) determines the analytical signal by removing negative frequency components and normalizing the signals from multiple sensors. A threshold energy sum algorithm is applied to the resultant signal in order to trigger alarms. If both occupancy sensors indicate a subject between the sensors and the processed signal is above the alarm threshold level for more than the target time, an alarm will sound. Alarm sensitivity is user configurable.

Following system validation, the system was mobilized to the White Sands Missile Range in the summer of 2009 for capabilities, limitations, safety, and operational testing. Operational Performance Testing was conducted to assess the performance of MAGUGS against two main metrics. The primary measure was the probability of detecting embedded metal fragmentation at a given distance in front of the sensor such that an alarm (audible and visual alert) was generated. The secondary measure was the ability of the device to operate without generating false threat signals when no subject was in the primary scan zone (FAR in false alarms per hour), and the ability to pass personnel with metal on their person no greater than a predetermined amount. This testing consisted of test subjects carrying targets having a variable metallic content through a simulated ECP at a range of walking speeds and with different levels of background and anthropogenic clutter present.

Specific details of the system performance have been documented by the Army Test and Evaluation Command. In general, the system reliably detected all types of targets tested including those containing minimal amounts of ferrous material. Both natural and anthropogenic clutter items resulted in false alarms. Range limitations were assessed and a preliminary set of standard operating procedures and tactics were developed to support follow-on operational field evaluations.

## 4.0 Operational Field Evaluation

Immediately following the capabilities and limitations assessment, we established low-rate initial production of 50 systems and a set of line-replaceable unit spares. The establishment of production facilities and completion of the first batch of systems was performed under a compressed 3-month period near the end of 2009. In early 2010, a subset of these systems were deployed to multiple theatres in support of Operation Enduring Freedom and Operation Iraqi Freedom. During the better part of 2010, the systems remained in-theatre undergoing operational field assessments at forward posts such as ECPs, combat outposts, and patrol bases as shown in Figure 5.

**Figure 5. Photos of operational field evaluation sites where SubtleMadness has been deployed.**

In 2011, SubtleMadness transitioned to support Operation New Dawn and then, subsequently, a subset of the systems were re-deployed in support of the Office of Security Cooperation-Iraq (OSC-I). Field service representatives indicated that systems have been in continuous use with limited combat loss. In some areas systems experienced damage due to heavy use in wet or submerged environments. Therefore, a waterproofing retrofit kit line-replaceable unit was established and delivered to forward operating areas.

## 5.0 Summary

Our overall objectives are to establish a PBIED detection system based on the SubtleMadness concept that reliably detects PBIEDs having a range of masses, metallic distributions and locations being carried through a checkpoint over a reasonable range of walking speeds. We have designed and fabricated a robust and user-friendly prototype for further operational assessments. To complete this objective we have conducted thorough sensor characterization and component selection followed by several rounds of iterative testing and design improvement.

The sensor components integrated in the system have proved more than sufficient for detecting even very small (<0.5 lb) metallic targets carried through widely spaced (many meters) sensors at all subject advance rates. Proven techniques leveraged from unexploded ordnance (UXO) detection experience were applied to sensor data to minimize false alarms while eliminating target misses. Clutter rejection techniques were used to further reduce false alarms. Some of the applied techniques included integrating additional sensors (electro-optical/infrared) into the system.

The system was made as robust and versatile as possible to accommodate variable operating environments, available electrical supply, and operator experience. This involved building a system capable of running off a wide range of DC and AC supplies or running on internal battery power when needed. Wherever possible the sturdiest and most robust components and materials were chosen or built, from environmental cases to power supplies, cables, and field-ruggedized PCs. The system performs extensive self test and self calibration functions upon startup and provides very clear directions for operation. Throughout testing, the user interface was simplified and refined so that an operator with no technical background can effectively use the system. At the same time, the system is able to provide detailed technical information about targets when required and can be easily upgraded to continue effectively detecting targets as PBIED metal content changes.

# 6.0 References

Billings, S. D., 2004. "Discrimination and classification of buried unexploded ordnance using magnetometry", IEEE Transactions of Geoscience and Remote Sensing, 42, 1242-1251.

Blakely, R.J., 1996. Potential Theory in Gravity and Magnetic Applications. Cambridge University Press. 464 pp.

Foley, J. 2005. "Naval Research Laboratory (NRL)/ Sky Helicopter Deployment to Lowry", Presented at SERDP / ESTCP / NAOC Technology Transfer Workshop, Aberdeen, MD.

Foley, J., Fonda, R., Pickner, M., Devries, L. and J. Davis. 2005a. "Helicopter Magnetometry Characterization: Integrated Technology for Wide Area Assessment", in Proceedings, Partners in Environmental Technology Technical Symposium & Workshop, Washington, DC.

Prouty, M., Smith, K., and R. Johnson. 2003. "Performance Considerations for Total Field Magnetometers." Proceedings of IEEE, Sensors 2003, (1), 483-486.

Schultz, G. and J. Foley, 2008, "Phase I SBIR Technical Report: A High-Speed Towed Magnetic Array for In-Road Detection of Improvised Explosive Devices Employing Optimized Magnetic Map Differencing", Joint Munitions & Lethality LCMC ACQ CTR AMSML-AQ- JA, US Army SBIR Project W15KQN-08-0067 Final Report.

Schultz, G. and Prouty, M, 2009, "Phase I SBIR Technical Report A002: Compact, Lightweight Magnetic Sensor for Small Unmanned Underwater Vehicles", Naval Sea Systems Command, US Navy SBIR Contract Number: N65538-09-M-0046 Final Report.