STIDP: A U.S. Department of Homeland Security program for countering explosives attacks at large public events and mass transit facilities

Christa K. Knudson*,a, Michael C. Kempb, and Nicholas J. Lombardoa

aPacific Northwest National Laboratory, P.O. Box 999, Richland, WA, USA 99352; bIconal Technology Ltd, St John’s Innovation Centre, Cambridge, UK CB4 0WS

ABSTRACT

The U.S. Department of Homeland Security’s Standoff Technology Integration and Demonstration Program is designed to accelerate the development and integration of technologies, concepts of operations, and training to defeat explosives attacks at large public events and mass transit facilities. The program will address threats posed by suicide bombers, vehicle-borne improvised explosive devices, and leave-behind bombs. The program is focused on developing and testing explosives countermeasure architectures using commercial off-the-shelf and near-commercial standoff and remotely operated detection technologies in prototypic operational environments. An important part of the program is the integration of multiple technologies and systems to protect against a wider range of threats, improve countermeasure performance, increase the distance from the venue at which screening is conducted, and reduce staffing requirements.

The program will routinely conduct tests in public venues involving successively more advanced technology, higher levels of system integration, and more complex scenarios. This paper describes the initial field test of an integrated countermeasure system that included infrared, millimeter-wave, and video analytics technologies for detecting person-borne improvised explosive devices at a public arena. The test results are being used to develop a concept for the next generation of integrated countermeasures, to refine technical and operational requirements for architectures and technologies, and engage industry and academia in solution development.

Keywords: explosives, IEDs, countermeasure, standoff, STIDP, large public events, crowds, test bed, person-borne, vehicle-borne

1. INTRODUCTION

The Science and Technology Directorate of the U.S. Department of Homeland Security (DHS) is responsible for researching and organizing the scientific, engineering, and technological resources of the United States and leveraging them into technological tools to protect the homeland. In support of Homeland Security Presidential Directive 19, DHS’s Explosives Division researches, develops, tests, and evaluates technologies to detect, mitigate, and respond to terrorist use of explosives in the United States. A priority for the Division is the development and testing of countermeasure architectures for detecting and interdicting explosives in free-flowing crowd environments. Promising prototype or commercial-off-the-shelf modules that meet the mission needs are adapted for large public environments, integrated into a system of systems, and tested in realistic operating environments.

DHS’s Standoff Technology Integration and Demonstration Program (STIDP) is designed to accelerate the development of integrated standoff and remote countermeasure architectures in crowd situations such as large public events and mass transit facilities. In alignment with National Planning Scenario 12, the program addresses threats posed by suicide bombers, vehicle-borne improvised explosive devices, and leave-behind bombs. The countermeasure architecture being developed uses modules such as sensors, people tracking, operator interface applications, and data management, all integrated into an open-architecture backbone.

*christa.knudson@pnl.gov; phone 1-509-375-3804; fax 1-509-372-4995; www.pnl.gov
The program uses a spiral development approach, which involves identifying commercially available technical solutions; modifying or maturing them to meet the architecture requirements of a free-flowing crowd; integrating them into a system of systems; testing them in live operational environments; and providing feedback to vendors, industry, and academia. Lessons learned from field tests are used to drive the evolution of the integrated countermeasure architecture. Gaps in countermeasure technologies and operations are identified as potential areas for research and development investments.

Detecting explosives at a distance in free-flowing crowds presents many challenges for countermeasure technologies and operations. Checkpoint screening is undesirable because detonating an explosive device in the midst of large queues of people results in a significant loss of life and damages to the venue infrastructure. That's why standoff detection and threat interdiction take place far from the presence of any queues or facilities. Another challenge with crowds is that countermeasure systems must detect a weak signal in a noisy environment. Systems must be able to be deployed in a wide range of venue types and layouts, including satellite parking, public transportation outlets, and multiple venue arrival areas and entrances. Crowd dynamics include wide variability in arrival frequency over short time periods, variant traffic flow patterns, crowd-blocking that could hide threats, and increasing crowd density at the approach to entrances. Sensors must be able to be located within the venue footprint with sufficient standoff distance, without impacting the flow of patrons. Detection systems also must provide sufficient room for law enforcement to interdict people of interest. Systems must work during high and low lighting conditions, all weather conditions, and within a fixed infrastructure that includes occlusions. Front and back screening of patrons is required, and the angle of approach may vary. The architecture must account for pedestrians walking by vehicles in parking lanes, loitering individuals and vendors, and people carrying children and objects. Current system concepts are labor intensive, with high lifecycle and asset protection costs.

This paper provides an overview of an initial countermeasure architecture design and results of a 2008 field test using that architecture at a live public event. The results are being used to guide the next stages of countermeasure development.

2. COUNTERMEASURE ARCHITECTURE AND VENUE FOR THE FIELD TEST

The most effective explosives detection approach for crowds requires multiple detectors embedded in a decision-making system, where each sensor measures different aspects of the same potential threat. A countermeasure architecture goes a step further, combining a suite of detection technologies that are operated and physically deployed as a system and integrated with the business operations of a venue. In the 2008 field test, the countermeasure architecture addressed person-borne threats in the form of suicide bombers and leave-behind bombs. The goals were to evaluate a baseline integrated system architecture for technology performance and cost-effectiveness in a live venue situation, to incorporate lessons learned into a long-range countermeasure architecture vision, and to provide meaningful feedback to vendors for spiral technology development.

The field test took place at the Toyota Center, a 6,000-seat, multipurpose arena in Kennewick, Washington (Figure 1). Though not as large as an urban arena, the venue represented the characteristics of a large public event: dynamic crowd flows with crowd density effects and multiple approaches.

For live operations, crowds arriving at the arena for five hockey games were screened during September and October of 2008. A privacy impact assessment was conducted and human-subjects testing was approved. Posted patron advisories allowed individuals to opt out of the test by using alternate entrances.
To deploy concealed object detection technologies, two discrete screening zones, 117 meters and 48 meters in length, were established along two highly used approaches to the venue (Figure 2). A 50-meter “safe zone” was established near the venue’s main entrance and box office, also serving as the area where video analytics were tested. The interdiction zone was established just outside the safe zone.

Figure 3 shows the infrastructure for the deployed countermeasure, and Figure 4 shows the technology systems. The field test used commercial technologies that would operate at a standoff distance of more than 20 meters and posed no public privacy concerns. Long-wave (8-12-micron) and mid-wave (3-5-micron) infrared cameras were deployed to detect concealed objects, such as a suicide bomber’s vest, by the thermal anomaly created when these objects obscure thermal radiation from the body (Figure 5).
Fig. 3. Overview of deployed countermeasure infrastructure. (IR = infrared.)

Fig. 4. Clockwise, starting from upper left: Mid-wave infrared camera, cameras on the Toyota Center roof, millimeter-wave radar probe, and long-wave infrared camera to detect concealed objects.
A millimeter-wave radar probe (lower left-hand corner in Figure 4), originally developed for standoff checkpoint screening, was used as a secondary sensor. The sensor head transmits and receives a low-power millimeter-wave radar beam, analyzes the reflected signal, and automatically determines whether a concealed object is present. The system presents the operator with one of three results: clear, indeterminate, or threat.

A stand-alone video analytics system also was deployed to identify leave-behind bombs and anomalous crowd behavior such as loitering (Figure 6). This system was used to test performance in a crowded outdoor environment and to benchmark people-tracking capabilities for future integration with the next-generation countermeasure architecture.

A number of interfaces were developed and modifications were made to the sensors to adapt them for the free-flowing-crowd environment and to integrate them as a system. The countermeasure included a number of system integration approaches:

- The infrared cameras and millimeter-wave radar probe were integrated via a tracking and handoff system that tracked and screened people with two detection technologies using different principles of operation.
• Technologies to detect leave-behind bombs and concealed objects, such as suicide bomb vests and belts, were simultaneously deployed to address the suite of person-borne threats.

• Multiple technologies to detect concealed objects were controlled and monitored through an integrated operator console (Figure 7). The integrated operator console provided the operators up to three different outputs from which a threat could be declared: an infrared camera, its accompanying visible-wavelength camera, and the millimeter-wave radar probe.

Both infrared and visible cameras were dedicated to each screening zone. The two zones shared the millimeter-wave radar probe, which was capable of screening either zone. As people entered either screening zone, operators used the cameras to scan for concealed objects. If a person of interest was identified as carrying a suspected concealed object, the operator would then conduct a second scan of the individual using the millimeter-wave radar probe. When the millimeter-wave radar probe was not being used for a secondary scan in either zone, it was used to randomly screen patrons in its home zone.

A target dispatch system was developed to assist operators in obtaining a scan with a second sensor. The target dispatch system allowed the operator to track a person (e.g., via infrared camera) and hand off the individual’s coordinates in space to a second sensor (e.g., the millimeter-wave probe), which would then automatically be positioned to scan the individual. The target dispatch system is an example of an open-architecture module that allows one sensor to obtain a target’s positional information and pass it among multiple sensors, thereby reducing operator workloads and providing them with multi-sensor data from which to make an interdiction decision. Though the target dispatch system was initially designed to track a single target, it was flexible enough to pass coordinates between many different sensor systems and provided valuable insights into the integrated use of orthogonal screening technologies. The use of the target dispatch system increased the speed of screening two zones with a shared sensor by reducing the time needed to accurately reposition the sensor between zones.

The field test was monitored using a commercial network video recorder software package that captured images from ten video surveillance cameras, the infrared cameras, and the millimeter-wave radar system. The software enabled recording, archiving, exporting, and playing back the captured images. Test team staff recorded key events, interdiction results, screen counts, and other testing and operational observations in the command center for subsequent analysis and future countermeasure design activities. Figure 8 shows the data acquisition and management structure.
3. FIELD TEST METHODOLOGY

The law enforcement officers who served as operators underwent countermeasure training to strengthen their skills in image interpretation, use of the sensors and integrated system, communications, and data collection. Before live operations, staff conducted vendor acceptance tests, integration tests, scoping tests, and countermeasure characterization tests over six weeks. The integrated suite of tests characterized the individual sensor performance and the general capabilities and limitations of the integrated countermeasure. Vendor personnel helped train the operators and were present during various testing activities.

The project team operated from a command center, a leased 12-ft-by-40-ft trailer located on the venue property. Two officer teams, each consisting of an operator and a spotter, operated the two infrared systems and the shared millimeter-wave radar probe; a fifth officer served as a supervisor. This configuration appeared to be the most effective based on multiple experiments conducted on ways to reduce staffing and optimize operator tasks and communications. All five officers were cross-trained on all systems and for all operational roles, performing all functions throughout the course of the field test. STIDP staff monitored the video analytics system.

Digital, observational, and patron survey data were collected during five well-attended hockey games. The data were used to characterize the venue (e.g., crowd arrival demographics and approaches), characterize the effectiveness of the
countermeasure architecture (e.g., people screened per hour, percentage of people screened, and nuisance alarm rate), and draw conclusions on seven key hypotheses related to screening of patrons at large public events.

A weather station was deployed to provide insights for system performance and situational awareness of environmental conditions for operations staff. The time of day (dusk) and time of year (fall) allowed data to be collected in a range of weather and lighting conditions, as well as testing with a wide range of clothing types and layers. Temperatures during testing ranged from 52 to 93°F, and weather conditions ranged from dry to rainy. Parking lot lights were augmented with trailer-mounted halogen floodlights for nighttime operations. This enabled operation of the people-tracking capability of the millimeter-wave radar probe and the visible-light cameras associated with the infrared cameras.

A series of simulated threat objects was developed for testing the countermeasure, based on an industry test protocol.[4] If one of the teams detected a potential concealed object during live operations, law enforcement personnel managed the interdiction process. Once a person of interest was interdicted, officers conducted a brief interview to document any person-carried objects or anomalies and communicated those interdiction results for data recording. Interdiction results helped operators and vendors understand system performance. People unknown to the operators and other command center personnel carried out red-team attacks on the countermeasure during live operations. Each red-team member wore a threat object and an outer garment and was instructed to follow the arriving crowd. The number of red team members varied from game to game. STIDP staff conducted after-action reviews of each round of testing to help reinforce threat object signature detection, operator protocol, and communications.

### 4. RESULTS

This section describes results for the characterization tests and live operations along with conclusions on test hypotheses. General results and lessons learned are presented without quantitative detection data.

The objective of the field test was to learn about integrating sensor technologies, rather than conducting side-by-side comparisons of equipment or systems. Benchmark performance tests in the operating environment were used to better understand technology performance relative to previous test and evaluation activities.

First, two statistically designed sets of tests were conducted to characterize the performance of the systems and to examine the effect of multiple layers of clothing. The characterization tests considered differences in concealment with outer clothing type, body types, benign objects, and crowd effects. Hired walkers were screened 338 times during 204 trials of singles and pairs; approximately one out of four walkers wore a threat object.

The most significant challenge during the characterization tests and the live operations was crowd density effects. During the live field test, Zone 1 crowd sizes averaged 23% singles, 44% couples, and 15% with groups of three, with the remaining 18% comprising groups of four or more people (Figure 9). Higher crowd densities resulted in blocking effects, lack of sufficient spacing between individuals, and lack of sufficient dwell time to make a threat determination.

An informal patron survey showed a high level of support for the operation, and very few patrons raised any concerns about being screened.
A number of hypotheses were tested during the field test, leading to the following conclusions:

- With five days of training, operators could detect concealed objects with acceptable accuracy. Additional practice resulted in a more effective operator team.

- Screening individuals with two orthogonal screening technologies as an integrated system improves detection and is an effective strategy to help make decisions about potential threats.

- Presenting screening results from the infrared systems and millimeter-wave probe on a single platform gave operators more information for interdiction decisions. Improving usability and situational awareness may significantly increase the benefit of an integrated operator console.

- The target dispatch system is a more effective way to reposition a sensor to a person of interest. A review of recorded video showed an instance where the target dispatch system acquired a person of interest in 7 seconds, while the manual acquisition of a person of interest for a different event took 23 seconds.

- The current architecture has a number of limitations that must be overcome for whole-venue screening, vs. the more limited zones used in the field test. These include line-of-sight issues such as parked cars, the number of approach angles, and standoff distance requirements that increase the number of sensors required.

- The video analytics system demonstrated the ability to track relatively large numbers of people simultaneously, but in a very limited area and under beneficial lighting conditions. To include video-analytics-based people tracking as part of the countermeasures architecture, it will need to handle larger coverage areas and performance under poor lighting conditions.

A number of challenges were identified related to countermeasure development for free-flowing crowds. These include overcoming crowd effects, preliminary screening of arriving patrons to identify the higher-risk ones, reducing operator workload requirements, improving situational awareness, enabling data fusion, using in-field spotters, ensuring countermeasure scalability and transferability, and improving sensors.
5. CONCLUSIONS

A test bed user facility was established to evaluate stand-alone or integrated explosives countermeasure technologies at large public events. The test bed significantly reduces time frames and costs normally associated developmental testing in live environments.

An initial countermeasure architecture for protecting crowds at large public events was developed and tested; lessons learned from these tests are relevant to protecting mass transit facilities as well. The architecture included integrated sensors to track targets and detect multiple types of threats, as well as ways to control and monitor multiple sensors. Vendors participating in the field test obtained unique insights into their sensors’ technical performance under live crowd conditions outdoors at a public venue. A team of law enforcement operators provided valuable feedback for concepts of operations and system development and usability.

Data and insights from live field testing are being used to develop the next-generation countermeasure architecture and technical requirements. The advancement of the person-borne countermeasure architecture will evolve with input from industry, academia, and other key stakeholders as it moves through the spiral development process. The architecture should articulate the various countermeasure layers and how they are integrated into a system of systems while addressing the screening challenges of large public events and mass transit facilities. The architecture also should be used to drive development of a roadmap that identifies critical technologies, technology gaps, and required research and development investments. The roadmap should be used to leverage research and development investments among agencies involved in standoff explosives research, development, testing, and evaluation.

DHS continues to engage industry in countermeasures development and maturation, including use of the test bed user facility at the Toyota Center. In addition, DHS also benefits from the integrated vision and recommendations of the Interagency Standoff Explosives Detection and Defeat Working Group, an international advisory group of government agencies whose missions involve countermeasure development and implementation.

ACKNOWLEDGMENTS

DHS’s Science and Technology Directorate, Explosives Division, oversees and funds the STIDP. Pacific Northwest National Laboratory manages the program for DHS, designed and implemented the countermeasure architecture and field test, and operates the test bed. Iconal Technology Ltd. serves as technical consultant to the field test and coordinates the STIDP with the European security community. The Interagency Standoff Explosives Detection and Defeat Working Group made recommendations on the components of the integrated countermeasures architecture and the field test. Vendors and other partners for the field test included General Electric Company, SET Corporation, The MITRE Corporation, and Thermal Matrix USA. Venue partners included VenuWorks, which operates the Toyota Center, the City of Kennewick, the Hanford Patrol, the Kennewick Police Department, and the Tri-City Americans. PNNL-SA-64793.

REFERENCES