

Airport Perimeter Security: Where we've been, Where we are, and Where we're going

Ann S. Barry and David S. Mazel, *Senior Member*

Abstract—Perimeter security at an airport requires disparate sensors to operate in concert to detect intruders; track them; assess threats; coordinate responses; (for example, human responders for investigation, or door and gate closings); gather evidence for law enforcement prosecution; and coordinate responses between law enforcement agencies. At present, no one system accomplishes all these tasks. Our work and development has evolved a system that meets these needs. In this paper we describe that evolution and show where we've been in system development, how that past has shaped our present deployment of systems and how our current work will lead to a complete solution.

Index Terms—perimeter security; radar and video sensors; data fusion; common operational picture, camera/sensor control policy; first responder directives.

I. INTRODUCTION

Perimeter security at airports is a difficult problem in a taxing and harsh environment. Systems must operate 24/7 and in all weather conditions. Airports are huge in physical size and often border on water;; nuisance alarms are ever present from surrounding wildlife; and what is more, physical installation space for sensors often is limited by FAA restrictions (Part 77) in runway proximity, placement, and height. These constraints are only relative to sensors. In terms of human interaction, the challenge is even greater. The system must be robust and user friendly so that operators can see relevant information and the display must not fatigue them. The interface must be intuitive and respond quickly to real-time data. These data may be numerous so that the system must handle all data quickly (often multi-faceted with different arrival rates and different resolutions) without any data loss, and without compromising on situational awareness. In short, the challenge is tremendous. How can we meet this challenge?

Our first step is to use organic – legacy - sensors. Many airports have air traffic ground surveillance radars which, if dual-purposed for security, are cost-effective and provide a broad-area surveillance sensor for the perimeter security mission. These radar systems can scan the entire airport, its perimeter, and beyond very rapidly, 24/7, and in all weather conditions. However, surveillance and detection are only the first steps in the solution, of course.

The next piece is to assess all detections: are they real intrusions or, nuisance alarms such as deer. Assessment may be accomplished with video cameras that an operator can train on the alarms. Better still, we let the system automatically point and drive a camera for assessment of a detected target. We allow these cameras to operate in accordance with airport policies, to be capable of hand-offs, and to be able to compensate for camera effectiveness so that best camera will be assigned to appropriate target. In addition, our system provides for video recording as evidence for prosecution.

Along with detecting, tracking, and assessing intruders, the system has to identify friends from foes. How can this be done? One way is to combine the information from multiple technologies—one that detects and tracks all targets, and one that detects and tracks only friendly targets—in concert to sort out the friends from the foes. An example is the use of GPS tracking of friends or with small identification badges that beacon the wearer's location combined with the all-encompassing detection ability of a radar system.

Next, the system has to fuse all these data sources to present a cohesive and clear picture of the state of security. Lest the operator be overloaded with data, the system has to make recommendations to the operator on what he should do based on the threats. Finally, the system has to alert first responders, pass data to the responders, and update each responder with information tailored for his immediate use. These are tall orders individually. Together they seem insurmountable.

Is such a system available? Yes. We call it SPAN, the Secure Perimeter Awareness Network [9]. To get there, we are taking an incremental approach.

II. DISTRIBUTED DEVELOPMENT

One way to build the system is to spend years writing requirements, designing the subsystems, writing software, testing hardware, integrating the pieces, and hoping the final system works. This approach is time-consuming, expensive, and will often lead to a system that is obsolete by the time it is completed.

Our (better) approach is to build some systems, test them, deploy them, and then add systems over time. We call this approach distributed development. It allows the system to evolve over a short time but in a way that uses the latest

A. S. Barry and D. S. Mazel are with Technology Service Corporation, 962 Wayne Avenue, Suite 800; Silver Spring, Maryland 20910; 301.613.3303 (Barry) and 301.576.2398 (mazel); Email {ann.barry, david.mazel}@tsc.com

technology, improves any past limitations, and fields working systems along the way. In the descriptions below, we show this process and how we have taken advantage of it. Figure 1 illustrates the idea; we will refer to that figure in the discussion below as we step through the systems in this figure.

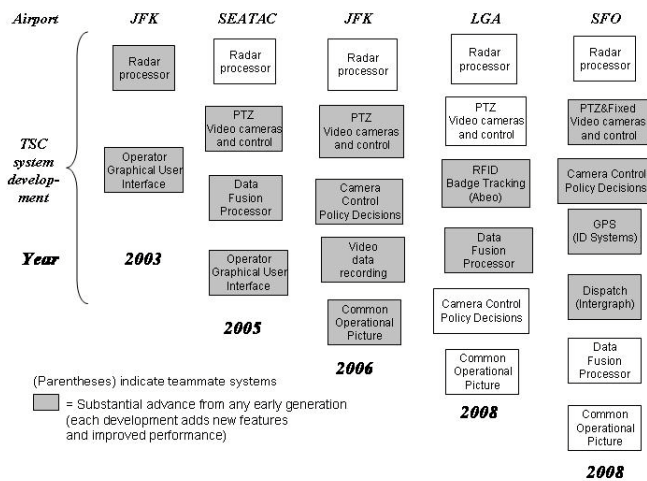


Figure 1: Security systems showing the process of distributed development.

Briefly, Figure 1 shows five systems at four airports: Seattle-Tacoma (SEATAC), John F. Kennedy International Airport (JFK), La Guardia Airport (LGA), and San Francisco International Airport (SFO). The boxes below each airport show the various systems we developed and deployed (or are deploying) at the airport. The shaded boxes represent new systems at an airport with respect to earlier installations while the unshaded boxes show systems that we have re-used from an earlier installation. The years at the bottom indicate when we fielded the system.

III. WHERE WE'VE BEEN

Our first system to discuss is our initial installation at JFK airport.

A. JFK Installation: The beginning

The first installation was a system at JFK where we deployed the radar processor and a Graphical User Interface (GUI) for an operator. This system was installed in 2003 and laid the ground for future developments and improvements. The radar processor and GUI are described below.

B. Mobile Ravin at SEATAC

Mobile Ravin (MR) was a deployment at the Seattle-Tacoma (SEATAC) airport. A detailed description of MR is in [3], [5]. We give a brief description of the systems for completeness and because these systems are used in subsequent installations.

Radar system sensor: The ASDE-3 (airport surface detection equipment) is the primary radar system for air traffic ground control of airplanes and vehicles within the terminal area of an airport. The radar operates in the Ku-band (15.7-17.7 GHz) in all weather conditions and can detect aircraft from 500-feet to

24,000-feet in range and up to 200-feet in altitude. The system wavelength, pulse width (40-ns), and rotational rate (1-Hz) are designed to resolve aircraft at a minimum cross section of 3-m^2 . It has an angular resolution of 0.25-degree and a range cell resolution of approximately 18-feet [1]. See [4] for a picture. To date, all our installations use the ASDE-3 radar.

Radar processor: The *ASDP* (Airport Security Display Processor) takes raw analog video signals of radar returns, processes them to reduce clutter, detect intruders, and display tracks. The ASDP decouples the air traffic control functions of the radar from any security functions [2].

Specifically, the ASDP system accesses radar video and timing signals from the ASDE-3 receiver. The ASDP Radar Signal Processor digitizes this radar video, performs detection processing, and range and angular measurement of detected targets. These radar reports are sent to the tracker. The RSP and tracker are referred to as the Security Radar Interface Unit (SRIU) and are housed in the same physical unit. The tracker then processes the radar reports into consistent tracks that are sent to the ASDP Display for operator viewing and interaction.

The ASDE-3 radar and ASDP systems are used in all the installations and development discussed in this paper.

Video processing and camera control for MR provided video data to the operator. It tracked objects within the field of view of each camera either passively or actively. Passive tracking was where the video system maintains location information on objects moving within a fixed field of view of a camera. Active tracking was where the camera follows a particular object and the video controller moves the camera to follow that object as it tended outside the field of view. Each camera was controlled by the operator directly or directed to follow and display a radar track [6].

The **Track Fusion Engine** (Data Fusion Processor) correlated radar track information with video track information. Whenever two tracks from these different systems reference the same physical object, the fusion engine produced a fused track. This fused track was displayed as part of the overall system display to eliminate redundant tracks and reduce the work load on the operator. In addition, a fused track will allow the operator to see a continuous track of an object even as the object moves beyond the detection of a single sensor. For example, if a tracked vehicle moved behind a building and therefore into a blind zone for the radar, a properly positioned video camera may maintain a track on that vehicle. Thus fusion allows gap-filling between blind zones of individual sensors.

The **Graphical User Interface (GUI)** was our display at SEATAC that showed a map of the airport, the radar tracks, and the video tracks. Figure 2 shows the GUI for MR. The airport has many installed video cameras around the facility; for this work we used two legacy cameras mounted on a

terminal roof (location shown in Figure 2) to track objects that the radar also tracks.

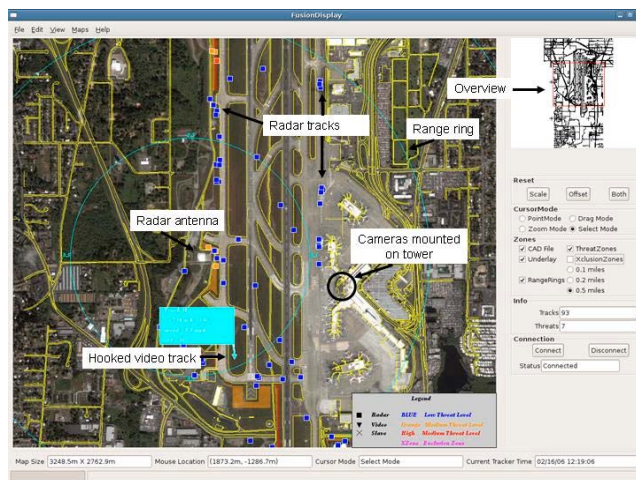


Figure 2: Mobile Ravin system display of radar tracks, radar and video camera locations, hooked track, range ring, and user interface.

Also in Figure 2 we show the radar antenna location, the location of the cameras, range rings for distance from the radar antenna, and the computer interface. The radar tracks are denoted by squares and video tracks are denoted by triangles. Figure 2 also shows information available to the operator such as track number, range and height of the object, and a track ID should he hook (select) a track.

The display shows an high-resolution image overview of the airport that may be zoomed-in on for close visual inspections of particular areas. The larger display shows warning zones (orange) and keep-out zones (red). Tracks that have never been in a restrictive zone are blue. Tracked objects entering a warning zone are shown as orange icons, and they are red if they have ever entered a keep-out zone. Red tracks constantly keep their color identification. The system will also notify the user of an intrusion (alert or alarm) with an audible alarm, thus allowing the user to pay attention to the system when possible action is necessary.

IV. WHERE WE ARE

A. SPAN version 1 at JFK International Airport

Our first step to the full SPAN system is our current system in operation at JFK International Airport, called SPANv1. Details may be found in [8] and we give highlights below.

SPANv1 at the Air Traffic Control Tower (ATCT)

The front end of SPAN ties in to the air traffic control radar. The signals from the radar are analog and consequently, we derive these signals and process them as close to the equipment as possible to limit any attenuation of the analog signals through the coaxial cable connections. Thus, part of our system necessarily resides near the radar and is, at JFK, in the air traffic control tower. All other installations have the ASDP/SRIU system close to the radar receivers as well.

Video cameras

For SPANv1 there are two Pan-Tilt-Zoom (PTZ) video cameras mounted on the air traffic control tower. Each camera has a video encoder that digitizes the video output and sends the encoded video over the IP-network to the Security Operations Control Center (SOCC) for display. Each camera is IP-addressable and controllable from the SOCC.

Network Video Recorder

The digitized video is also sent to digital video recorders. The video is recorded in a rolling buffer for 30-days. The resolution is 4-CIF (640 by 480 pixels) in NTSC interlaced format. This video can be searched based on date-time stamps, written to a DVD for long-term storage, and is of suitable quality for use in legal proceedings.

SPAN at the Security Operations Control Center (SOCC)

The JFK SOCC is manned constantly and is the command center for security operations at JFK airport. There are three fundamental SPANv1 subsystems in the JFK SOCC: The ASDP GUI workstation, the Common Operational Picture (COP) and the camera control system.

ASDP GUI Workstation

The ASDP GUI workstation was described at a basic level above in the discussion of MR. Basically, at JFK it serves as the head-end display of the ASDP radar surveillance, detection and tracking sensor subsystem.

Common Operational Picture (COP) workstation and display

The COP is a system hosted on a Windows PC with a large screen display that integrates all sensors to a unified display for situational awareness and command and control operations. In normal operations, the COP displays a layered map of the airport with threat zones overlaid. Typically, only threat tracks as well as the video from each camera are constantly displayed. The COP may display all tracks, threat and non-threat, as desired. It may interact with the GUI but it can also work independently of the GUI.

With the COP, the operator may employ various control functions such as hooking tracks for data (threat level, velocity of the track, location within the airport grid); hiding tracks; showing specific tracks from the GUI on the COP; adding sticky notes; and changing display parameters among others. The camera footprints are displayed on the COP to give an intuitive indicator to the operator of camera location and the width of these footprints changes automatically to indicate the zoom setting of each camera.

Figure 3 is a screen capture of the COP display annotated to give an indication of its functionality. The display shows a photographic overview of the airport that the operator may zoom-in to see particular areas in detail. The larger display shows warning zones (orange) and keep-out zones (red). Blue icons represent objects tracked by SPANv1 that have never entered a keep-out zone. The SPAN system will issue an alert (warning) or alarm (requires action) if a tracked object breaches into one of the user-defined alert or alarm keep-out

zones. If this occurs, the SPANv1 will issue an audible alert/alarm, and will change the color and shape of the tracked object icon on the COP display. An orange icon represents an alert while a red icon is an alarm. Once a tracked object has been declared an alarm, its icon will remain red as long as the system continues to track that target. The COP is quite extensive in its usability and functions, see [8] for more details.



Figure 3: The Common Operational Picture display shows a high resolution map with camera videos that form a single integrated security picture. Camera footprints are color-coded to match the associated video windows and keep-out zones are delineated by level of alert (yellow is warning, red is alarm). Information for a hooked track is shown in the call-out bubble.

Camera Control (Briefly)

To control the cameras, we developed a camera control system that:

1. Implements airport security policy for investigation and tracking of intruders
2. Allows each camera to be automatically controlled by the system
3. Allows each camera to be manually controlled by the operator
4. Is extendable to multiple cameras without changes to the existing implementation
5. Is fault tolerant so that a “bad” camera does not adversely effect control of any other camera and may be compensated for with a different camera
6. Handles camera hand-offs as a target moves between different camera field-of-views

Part of the airport policy we implemented, for example, is that when an intruder crosses a keep-out zone, say a boat comes too close to the shore, the system will automatically select the best available camera, slew that camera to the intrusion, and follow the intruder.

B. ASDP with Bio-RFID badges and video: LGA

Our system at LGA is currently under development with installation scheduled within a few months. However, the basic subsystems are shown in Figure 1. Because the system

is still in development, we will present the architecture at the conference.

The radar is the ASDE-3 and the signal processing is the same as earlier systems. The additional camera is a Pelco Esprit with 35-zoom with a similar connectivity as SPANv1.

What is new is that on the Air Operations Area there is a constellation of antennas that communicates with specially designed Bio-RFID badges. The badges allow communications between each one and the antenna constellation with position data of the badges going to the COP. The badges allow the system to track the wearer as well as require badge holders to authenticate themselves. At the COP the operator can request a user to authenticate his badge with a fingerprint. Notification to do so is indicated on the badge by either a flashing LED or an audible beep.

Identify Friend of Foe (IFF) at LGA

When we couple the radar system that sees all targets with the badges that track authorized personnel, we have an IFF system. How does this work?

The IFF system works by exclusion. The radar sees all targets on the AOA whether a target has a badge or not. When the radar sees a target, the system will track that target. The Bio-RFID badges tell the system where authenticated (or authorized) users are. If we spatially subtract the authorized personnel from the radar tracks of all people, we are left with the unauthorized personnel on the AOA. (In reality, the system is identifying unknowns, not necessarily foes. However, this is the first implementation of such functionality for any perimeter security system.)

Data fusion

The IFF process requires the system to match radar tracks with badge tracks. To accomplish this we have redesigned what is now a newly developed track fusion engine (data fusion processor) that we used earlier in MR. In brief, the Bio-RFID cards provide the system with position data. From these position estimates, we develop a track on the badges with a Kalman Filter. The new track fusion engine compares tracks from the Bio-RFID tracks to the radar tracks. This comparison

1. Eliminates from consideration any tracks that are far apart spatially.
2. Compares tracks that are close spatially in terms of position and velocity
3. And if the tracks are close in a statistical sense (Mahalanobis Distance) then the track fusion engine correlates those tracks.
4. It updates these correlations with every new set of track updates in real-time and for over 100-radar tracks per second.

COP

The final piece at LGA is a Common Operational Picture (COP) that is operator controlled. This COP is similar to the SPANv1 COP with added functionality to interact with the

Bio-RFID badges for positional data and authentication requests and responses. Other features will be presented at the conference.

C. ASDP with GPS, Multiple cameras, Dispatch: SFO

Figure 1 shows the systems for the SFO development. As in the other installations, the radar system is the ASDE-3 with our ASDP/SRIU in place to process the radar returns to tracks.

Existing PTZ cameras

Unlike earlier efforts where the cameras were acquired for our work, this installation has existing Pelco cameras installed along parts of the perimeter of the airport. We are interfacing our system to these existing cameras. This illustrates one of the features of SPAN—it is capable of using legacy equipment so that existing sensors may be integrated to the whole system.

The camera integration will not only use the existing cameras but will also go through the existing camera infrastructure. Currently, the Pelco system at SFO uses Pelco data management priority controllers. Our installation will also use these devices and in a seamless manner so operators can continue to work as they always have without interruption. Naturally, our integration of the cameras will implement airport camera control policy to dictate when to slave to a track, slew to targets, and how to prioritize camera operations.

GPS tracking (Blue Force) with Data Fusion

Our system will also integrate GPS position data from vehicles (from ID Systems, Inc.) that operate on the Air Operations Area. As part of this pilot program, three vehicles will be equipped with GPS position systems. The position data will be sent to our system where we will implement a system similar to the RFID badge tracking at LGA. The GPS position data will be sent to a specially designed Kalman filter for tracking. The output of this filter will be sent to our Data Fusion Processor (Track Fusion Engine) for correlation to any radar tracks. If there's a correlation, the operator will be notified via the color and shape of the tracked icon on the COP, and he will know the position, identification, and speed of the target.

Dispatch system

Our system will not only take in data, process them, and display them to the COP for operator responses and interaction, but we will also transmit data to a computer-aided dispatch system (by Intergraph Inc.). Our data will allow Intergraph to display some of our radar tracks, and allow them to see where the PTZ cameras, under our control, are pointing.

Video Analytics

The COP at SFO will take in video analytics data of intrusions that cross the field of view of fixed cameras (not shown in Figure 1). Vidient Inc. is implementing a video analytic system and they will pass alarm data to the COP where it will be displayed.

Common Operational Picture (COP)

It is worthwhile to note the various data that our COP will display and interact with for this work.

1. Radar tracks from the ASDE-3 at possible data rates of over 100-tracks per second
2. Simultaneous control and tracking of targets in and around the perimeter for real-time assessment using up to eight PTZ cameras
3. Tracking of GPS equipped vehicles with data fusion for correlation
4. Data feed to a computer aided dispatch system
5. Real-time display of the airport perimeter, environs, and video cameras in a single integrated picture

V. WHERE WE ARE GOING: SPAN

We have described four perimeter intrusion detection systems for airports through the country. What is our goal?

Figure 4 shows the systems we envision in a full deployment of SPAN [7],[9]. The clear boxes are systems that we have deployed at one of the sites discussed above while the shaded boxes are new systems for integration into subsequent deployments.

Sensor Input

The sensors are all technologies we have employed earlier except for fence sensors (and not shown, seismic sensors). These are both point sensors that show an intrusion happened at a point and time but without any updates for tracking. Integration and response is similar to the video analytics of an intrusion crossing a fixed camera scene: the system detects the intruder, notifies the COP, the operator may respond, but there are not necessarily additional sensor detections of this intrusion. Integration of these sensors to our existing system development is straightforward.

The core functions have (mostly) been implemented save for the event fusion and decision making and communications to first responders. (Sensor priority and policy engine relates to our camera control policy that we have already deployed.)

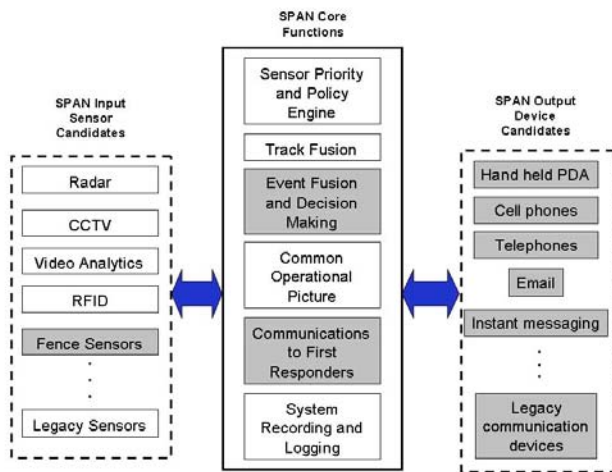


Figure 4: SPAN overview and systems. The clear boxes are systems we have already deployed while the shaded boxes are soon to be deployed systems.

Event Fusion

Event fusion combines spatial and temporal alarm events such as sensor alarms, access control breaches, and track activity, to form a consolidated event from tracked (radar) and non-tracked (point sensors such as fence sensors or access control) incidents. Decision making is a computer aided program that applies airport security doctrine to events to produce a recommendation (or even send an automatic response if desired) to an operator for action. This fusion, by the way, is not data fusion above where track data are correlated but is a method of combining individual events into a coordinated response. We intend to add this capability in future deployments of the system.

First Responder Communication

First responder communications are part of the core functions and have a large share of the overall system (see Figure 4). The purpose is that the operator in front of the COP can dispatch responders to intrusions and update them on situational variations. The operator can send the responders relevant data, such as the current location of the intruder, information about the physical area (fuel depots, high value targets), other responders (blue force tracking) already present or en route, and videos of intruder actions.

Notification to superiors and other authorities

In addition to notifying responders, the system will notify superiors who may have to coordinate responses within the airport, deal with outside authorities, and in general coordinate and update outside officials. Devices listed in Figure 4 will serve these functions.

Scalability/Command and Control

As a final note, SPAN is designed as a scalable solution so that it can be deployed in a limited capacity, say, as we have done in the past, or as a large, fully integrated system as we plan to do in the future. One implementation does not prohibit the other in its development. Further, we see SPAN as a common point within an airport for command and control of

the sensors, the situational awareness for operators, and the coordination of responders and other agencies as need be.

VI. CONCLUSIONS

SPAN is our system for detection, tracking, and response to intrusions in and around an airport. It is continuing to undergo distributed development so that systems are developed and deployed at different times and locations with the end goal of a fully integrated, tested, and deployed system.

ACKNOWLEDGMENT

The authors acknowledge Mr. Mark Torbeck of the Transportation Security Administration/Transportation Security Laboratory for technical oversight; Mr. Patrick O'Brien, head of the security at the Seattle-Tacoma International Airport for support with Mobile RAVIN; the Technical Support Working Group for support in the original development of the Airport Security Display Processor system at the John F. Kennedy International Airport, New York, and for support and funding of SPANv1 at JFK. We also gratefully acknowledge the Port Authority of New York and New Jersey for their continued support and hosting of SPANv1 and, in particular, Mr. Al Graser, Ms. Jeanne Olivier, Ms. Maria Chen, Ms. Novellete Roberts, and Mr. Saurabh Pethe for their continuing support as we deploy at LGA. Ms. Kim Dickie, assistant deputy director, aviation security at SFO, is kindly acknowledged for her support and assistance.

REFERENCES

- [1] Barry, et al., "ASDE-3 Radar Siting and Analysis Security Study," Final Report, TSC-W111-079, Oct. 2000.
- [2] Mark Bond, *Airport Security Display Processor: Software Requirements Specification*, TSC-W234-020, March 2005.
- [3] *Mobile RAVIN Design Document*, TSC-W282-010, October 2005.
- [4] ASDE-3 antenna photograph available at: <http://www.tsc.com/images/contentimg/ASDP2.gif> last accessed March 6, 2008.
- [5] David S. Mazel and Ann S. Barry, "Mobile RAVIN: Intrusion detection and tracking with organic airport radar and video systems," in the *Proceedings of the IEEE International Carnahan Conference on Security Technology*, Lexington, Kentucky, October 2006.
- [6] *Mobile RAVIN Design Document*, TSC-W282-010, October 2005.
- [7] Ann S. Barry and David S. Mazel, *Secure Perimeter Awareness Network (SPAN) System Requirements Specification*, Technology Service Corporation, April 6, 2007.
- [8] Ann S. Barry and David S. Mazel, "The Secure Perimeter Awareness Network (SPAN) at John F. Kennedy International Airport," in the *Proceedings of the 41st IEEE International Carnahan Conference on Security Technology*, Ottawa, ON, Canada, October 9-11, 2007.
- [9] Patent entitled, *Security Architecture and Methods for Providing an Improved Integrated Security Network for a Facility*, Ann S. Barry, inventor; Date of regular patent application: 1 February 2006; Pending.