On Airport Perimeter Security

1. Introduction

Security of facilities, infrastructure and strategic assets at airports and in the vicinity of airports is an integral part of a total aviation perimeter security model. Enhancements to the security posture at airports provide the foundation for valid requirements that influence the fiscal planning to realize a level of physical and electronic protection that can logically evolve as the requirements for new features and functions change. This security spans a range of integrated technologies including perimeter sensors and fencing, command and control and communications infrastructures, dispatch, cameras, radars, and electro-optics, and access control. The perimeter intrusion system is linked with radar and video displays and audible warning signals to alert and visually geographically locate, alert, and continuously track incident events. The principal purposes of the system are to improve situational awareness for on site security personnel and to report and record probable security incidents. The monitoring and recording capability also facilitate safety investigations and litigation reviews. This white paper considers a ubiquitous candidate system for airport perimeter security, briefly describes a concept of operations for that system, and identifies a system architecture for perimeter security protection.

2. System

A candidate airport perimeter security system provides a complete solution to securing high value aviation assets, from airport terminals and AOA, to the airport perimeter and beyond including buildings, plants and facilities. The surveillance system integrates a broad range of perimeter and access control technologies into one cohesive configuration that is monitored and controlled through a common command post. Ground radar sensors and electro-optic surveillance cameras create a visible or “virtual” perimeter protection area. Wide area surveillance will be performed in real time from a number of locations simultaneously using standard multicast video transmission technology in a Metropolitan Area Radio (MAN) format. Open standards transmission and encryption using wireless radio technology is in compliance with the range of transportation related technologies identified in the Intelligent Transportation System (ITS) architecture enhances system operation and performance. Networking of command and control, and monitoring would provide the following uses and benefits:

- **Detection –** vehicles, wildlife, and personnel attempting to enter the protected perimeter of the airport
- **Warning –** local and remote notification
- **Incident Prevention –** attempted intrusions detected early enough in the reaction cycle to take action prior to the incident
- **Enforcement –** Local security personnel and airport operations centers would use the perimeter monitoring system to enforce traffic control laws

- **Verification –** redundant direct observation of the perimeter would provide a continuous verification of the operation and safety of control equipment
- **Reporting –** security personnel at the site and various agencies would be provided with all available information concurrently on any perimeter breach incident (common operating picture)
- **Documentation –** Onsite and remote recording equipment would provide complete information
- **Surveillance –** right of way and high security property would be continuously monitored as well as detection of situations that might endanger public safety such as trespassing, terrorism related activities, or vandalism

This perimeter intrusion system uses proven, commercially available technology to significantly enhance area security and presents a flexible, scalable response in mitigating intrusions and trespasser threats. The system provides an unobtrusive surveillance capability and employs low cost systems technology which could reduce on-site personnel. It is important to note that the intrusion detection technologies can be engineered as a function of the system requirements in various combinations to achieve the required level of perimeter protection. In addition they can be integrated with existing technologies and evolve as requirements change to reflect new or modified threat scenarios.

3. Concept of Operations

The perimeter of an airport is some combinations of roads, rural pathways, coastlines, waterways, urban areas, and borders. The basic perimeter protection system concept is to detect intrusion attempts, however small, using some combination of low cost, low power ground surveillance radars, all weather video surveillance cameras each with intelligent intrusion detection capabilities, smart fencing, optical detection, and buried fiber cable. The detection information from these systems is fused and superimposed on a video picture of the monitored area to provide information on the precise location or locations of the attempted intrusion. Figure 1 shows an overview of the concept with a logical command and control. The system continuously and passively monitors the perimeter and other designated areas using rules-based detection methods to eliminate the need for constant human monitoring of video screens. On detection of an intrusion attempt, alert warnings in the form of radar surveillance and video displays and audible warning signals are presented directly to security personnel at a command post/operations center, and to local law enforcement or security offices as specified by procedure and/or protocol.

Video cameras with digital zoom and pan/tilt/zoom (PTZ) capabilities allow operators to manipulate the video display. The radar outputs a simple contact closure alarm on detection which activates the camera control mechanisms. Radar is used as the primary sensor because of its superior performance in varied weather conditions and wide area detection capabilities. Forward Looking Infrared (FLIR) technology is also a candidate within the spectrum of detection components. The cameras (see Figure 2) have separate intelligent intrusion detection capabilities for redundancy and capabilities to augment and verify radar performance. The cameras would provide a simple, easily understood output showing what the radar detects. Object detection sizes are dependent on the capabilities of each intelligent detection system but would be set so that each system compliments the other. Detection rules and system capabilities would be designed to resolve object sizes to whatever range is necessary to adequately survey the airport perimeter.

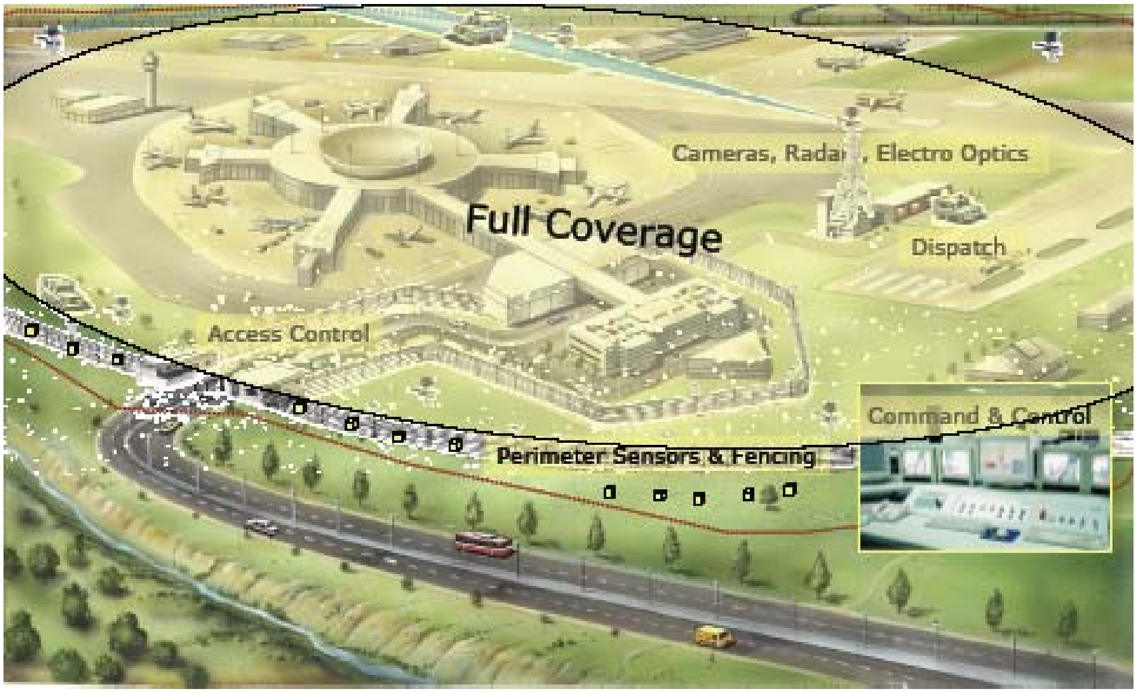

Figure 1. Concept Overview. Airport perimeter full coverage security is provided by a combination of integrated sensor technologies fused through a command and control suite, and augmented by secure, wireless, wide area communications.

Upon detection by a sensor, alarm conditions are generated and live video will be transmitted to the security command post/operations center. Manual control of the cameras may be accomplished at any time by the security personnel or other authorized users. A display and alarm system connected to all monitoring stations will be integrated into the existing physical security systems. A local 'black box' will be used for incident recording and recording of environmental conditions at the time of the incident. The system will be primarily powered by batteries charged with solar panels to limit the amount of external infrastructure needed for system operation. This will also allow for installation in remote locations. Tamper control and intrusion detection sensors will be used for self-protection of the system.

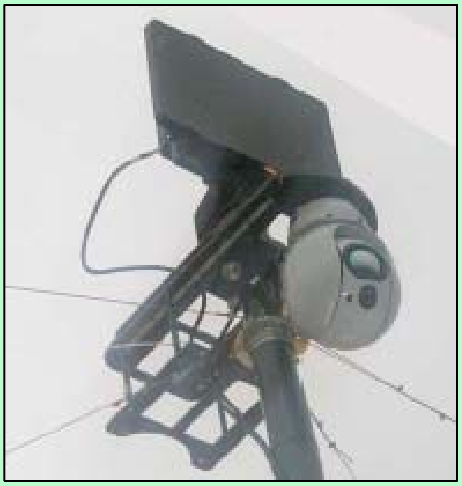

Figure 2. Wide Area Ground Surveillance Detection Suite

Smart fences provide warning, detection, and alerting with automatic camera slaving and incident recording. Three possible scenarios can be addressed. The first simply uses a vibration detection fence system and relies on that detection to signal control and monitoring stations that an event has occurred. The second, shown in Figure 3, introduces video motion detection (VMD) cameras in the smart fence to provide an advanced warning of an impending intrusion. Scenario 3 integrates both VMD and radio frequency (RF) sensing to provide an all-weather warning system.

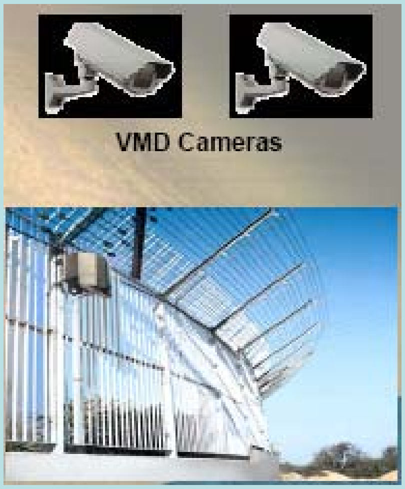

Figure 3. Smart Fencing With VMD cameras.

Optical detection systems, including buried fiber optic intrusion cable, provide an additional level of protection where the use of cameras including radars is not practical. They are either fence mounted or buried in the ground. The fence mounted versions are self calibrating, with variable sensitivity settings adjusted to reduce false alarms caused by high winds, lightening, or blowing debris, including snow. Automatic recalibration in the order of seconds is designed to provide alarms on continued intrusion attempts as could occur from animals.

Buried fiber cable (see Figure 4) provides an invisible barrier to intruders of many sizes and shapes depending on the detection sensitivity. It does not, however, classify the type of intruder such as human versus animal versus a vehicle such as a bicycle. It simply indicates the presence of a potential intruder. The cable is placed into a narrow trench along a path on the perimeter. The system is based on highly sensitive interferometric sensing techniques. If the fiber cable is disturbed for any reason by changes in pressure caused for example by humans or animals walking in the area, the optical transmission characteristics of the cable change and a sensor is activated. Using well known time domain reflectometry techniques, that is changes in the characteristics of the reflected waves in the transmission line (fiber cable), the location of the disturbance can be isolated to within tenths of meters. It is integrated with VMD or FLIR cameras having PTZ capabilities so that an intrusion can be localized. The benefits of a buried fiber approach are very wide area coverage, high sensitivity, electromagnetic immunity, ease of installation, and long term reliability. This technology provides an excellent solution in combination with smart fencing for deployment in environments where camera and radar technologies can not be effectively mounted to obtain the needed coverage. Dense foliage or forested areas with multi-sided geometries, in lieu of long runs, are examples.

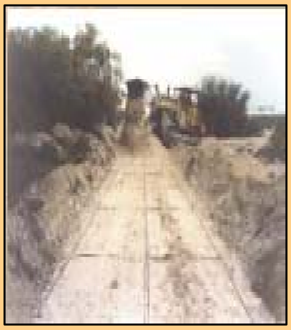

Figure 4. Buried Fiber Optic Cable

Existing command, control and communications (C3) at the airport are augmented to accept the perimeter sensor inputs to provide multi-sensor integration, analysis and semi-automated camera control, and communicate with either first responders that investigate and contain the intrusion or provide activation of other tactics that serve to ward off animals viewed as intruders (see Figure 5). The command structure is derived from data and intelligence developed by the various integrated sensor suites. This provides a means of management control of suspected interdictions. Using available data, control is synthesized and exercised by operators to provide operational direction to first responders or to invoke other tactics.

Figure 5. Example of a Mobile Crisis Command, Control, and Communications (C3) Center Integrated with Airport C3 facilities and capabilities

4. Technical Architecture

Physical security, alarm reporting and event recording could be readily introduced or enhanced at minimal cost by employing state-of-the-art capabilities using security and surveillance advances in the application of Defense and Homeland Security technologies. This would lead to an all-weather, wide-area surveillance, detection, alerting, and incident tracking and recording perimeter intrusion system for the protection of critical infrastructure and physical assets at an airport and on its perimeter. Because of the range of environments constituting the perimeter of an airport, the perimeter intrusion system would be a multi-sensor suite composed of any subset of the following proven technologies all recorded and managed from a computer-based control system. As shown in Figure 6, the system architecture will have the flexibility to incorporate the integration of additional technologies as they become available or desirable. Hardware, software, communications, and network interfaces will be designed and thoroughly tested in order to accurately portray system requirements and support needed capability. The following are highlights of the perimeter security system as part of an overall aviation security concept.

- Integrated and overlapping ground surveillance radars, including forward looking infrared (FLIR) for open and long-range coverage,
- Short range localized ground surveillance detection using radio frequency sensors with target identification,
- All weather video surveillance systems providing full, seamless coverage of the perimeter line and areas either side of the demarcation line,
- Smart fencing using combinations of vibration detection, cameras with pan/tilt/zoom capability, and radio frequency, warning detection and alerting with automatic camera slewing,
- Optical detection systems using fence mounted cable that is self-calibrating with variable sensitivity settings to provide detection of fence scaling, cutting, lifting fence fabric, or going over the top (ladder scaling)
- Buried fiber optic intrusion cable using interferometric sensing techniques and characterized by electromagnetic immunity, high sensitivity, and long-term reliability.

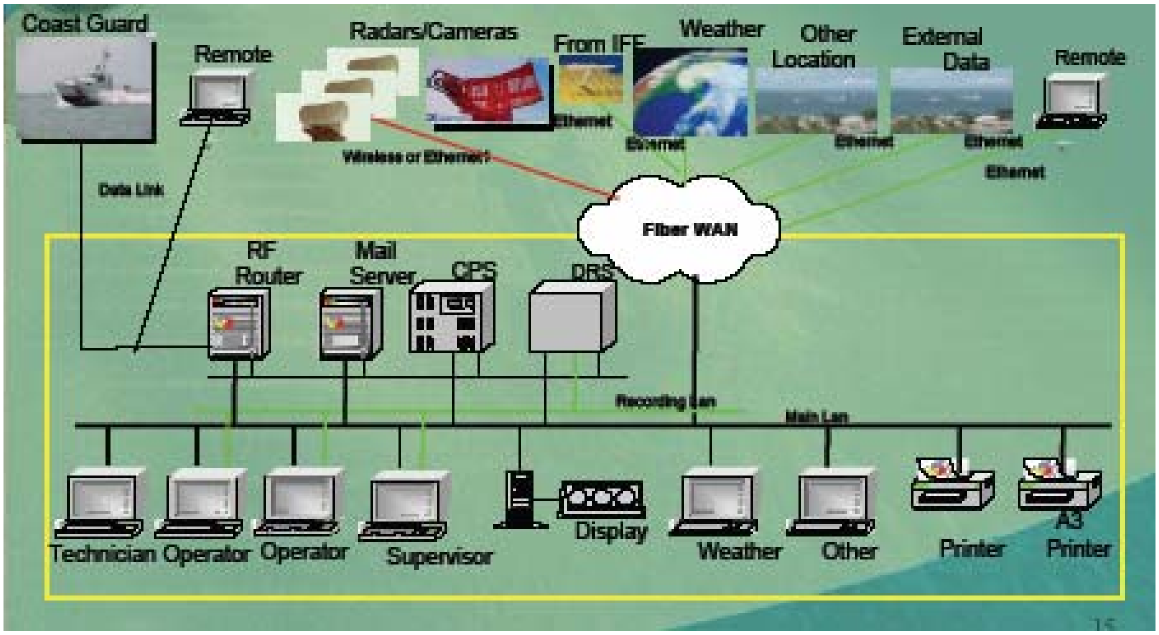

Figure 6. Technical Architecture. Sensor Suites To Countermeasure Potential Intrusion and the Supporting Functional C3

5. System Integration

Small light weight advanced ground surveillance radars and video cameras will monitor the perimeter, and the area either side of the perimeter using an integrated local rules-based intelligent intrusion detection system interface. Smart fencing and buried fiber cable will provide unique detection capabilities where other detection forms are either not workable or economically viable. Technologies are combined and deployed to match the requirements levied on the perimeter protection system. The number of radars and video cameras is dependent upon the size and configuration of the local perimeter. The ground surveillance radars are active detection sensors with specific detection zones based on the physical configuration of the area to be monitored. The radars detect intrusions and cause specific cameras to electronically move to the location of the detected intrusion. The cameras will have an independent capability to detect security breaches and will pan across its designated monitoring area as a secondary detection system to augment the detection capabilities of the radars. They will be used in conjunction with smart fending and buried cable. Initial design of the system components and inspection of the designated installation sites will be accomplished to determine the degree of integration and capabilities needed at each site on the airport periphery to satisfy the broad range of technical requirements and environmental conditions.

The required technologies can be integrated with existing protection mechanisms so that the system can logically evolve to take advantage of technical and economic advancements as they become available. For example, a buried fiber cable solution can be integrated with an existing smart fence approach since the cable is the common dominator, and modulation of the cable waveforms is the mechanism used in detection of potential intruders at a control point.

The projected system components will require minimal development for integration. The majority of current projects in the Homeland Security arena where cameras and radars have been integrated for reliable detection capabilities meet the operational requirements envisioned for perimeter security.