A Senstar Corporation White Paper

119 John Cavanuagh Drive
Carp, ON K0A 1L0
+1.613.839.5572
www.senstar.com

Airport Perimeter Security

By: Jonathan Murray
November 2012

November 2, 2012

Contents

Background

Security in airports has always been a high priority with high visibility, yet the perimeter surrounding the airport was, and still is in many cases, neglected.

If an airport does have full fence coverage, it is usually a dumb fence, without any detection capability. Airports are investing billions on the obvious security measures we see as members of the travelling public – screening, cameras and x-ray machines; yet the fastest way to the runway and airplanes – the perimeter - is left open.

Terrorist threats at airports have almost become the standard by which we measure threat scenarios, but what about the random threats?

In July 2012, a man in Salt Lake City, Utah scaled a razor-wire toped perimeter fence, using simply a rug, and stole an idle 50 passenger jet. Fortunately this plane never left the ground, but it did raise obvious concerns over airport perimeter security.

Another example is that of a truck working in an airport's segregated area and by mistake, driving in the wrong direction into the runway. This scenario could easily occur and turn a minor security violation into a catastrophic safety event. This is indeed the case at airport environments – a small trigger can light a huge fire resulting in a massive negative worldwide effect.

As we know, any security chain is no stronger than its weakest link, so each segment and sector of the perimeter must be secure enough to ensure the entire perimeter is protected.

Concept of operations

Typically it is recommended to start with a full security concept - no band-aid approach to weak elements of the site. This step requires professionals to analyze threats and match them to the right CONOPS (Concept of Operations) – define areas demanding high security versus lower security priority sections; identify the location of your command and control center, and determine whether more than one is needed. Identify where first responders are located and how long will it take them to respond to an alarm. If the perimeter has been breached, how long will it take to respond effectively and intercept the intruder?

Once these elements have been defined, a tactical plan can be developed whereby the best combination of technologies and processes for each section of the perimeter can be tailored to the PIDS (Perimeter Intrusion Detection System).

The recommended solution

The simple answer to the challenge of perimeter security at an airport (or any similar critical perimeter for that matter): a combination of smart fences and barriers, supported by a mix of long range surveillance cameras with smart cameras (i.e. equipped with outdoors IVA – Intelligent Video Analytics). And last and very important - a fast and responsive mobile force with a centralized PSIM System (Physical Security Information Management).

Additional sensors and tools may be needed to close specific gaps unique for each airport. Ideally, an airport should have a minimum of a two layered PIDS solution installed, and some airports (like Indira Gandhi International Airport in Delhi, India) choose four layers for better confidence.

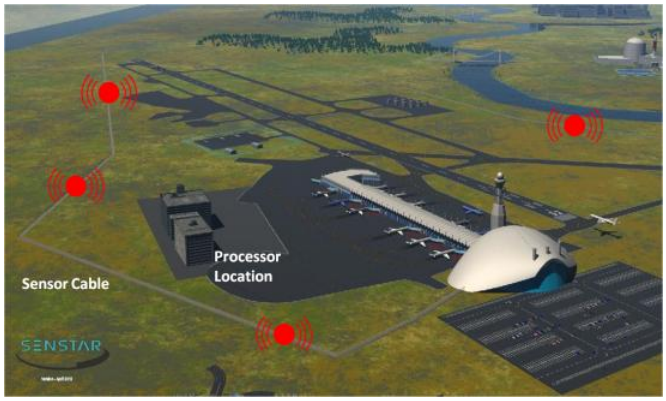
Recommended sensor technologies

Taut wire – the Cadillac of the fences as it is a hybrid system of sensors weaved into a barbed wire fence. This is the only fence that has, in all weather conditions, guaranteed performance with demonstrated high Pd (Probability of Detection) and almost zero FAR (False Alarm Rate). This is an excellent choice of technology where false alarms cannot be compromised. It can serve as a standalone barrier with no additional verification tools (like cameras), although additional layers will increase performance.

Fence mounted sensors – There are a few technologies that support these applications – be it microphonic copper cable, fiber optic sensors, vibration sensors or even seismic sensors. All of these systems are ideal as add-ons to existing fences, since in these cases most of the investment is already done. Customers need to be aware that fence mounted sensor performance requires, in most cases, a secondary verification tool. Performance is not always guaranteed and sometimes depends on the quality of the installed fence. The same sensor will perform completely different on a loose fence versus a rigid tightly installed fence. In the case of airports, covering a huge landscape, this may create a quite a few nuisance and false alarms per day. Some of the available sensors can locate the intruder within a sector to the level of a few meters. For airports, this ranging feature is not critical since airports are relatively open and flat, and thus with the inherent delay caused by a fence, typically 100 to 150 meters resolution of detection is plenty.

FiberLR

FiberLR's advanced fiber-optic technology provides up to 16 km (10 mi.) of perimeter protection when installed on fences, buried, or mounted on a wall. For protection of buried pipelines against ThirdParty Interference (TPI) FiberLR provides up to 48 km (30 mi.) of protection.



FiberLR accurately locates intrusions even when there are multiple simultaneous intrusions and even in the presence of background environmental noise that would overwhelm the location capability of other sensors.

FiberLR's resilient design allows detection to continue right up to the point of a cut in the sensor cable. When installed in the closed-loopconfiguration FiberLR protects the full perimeter even after a cable cut.

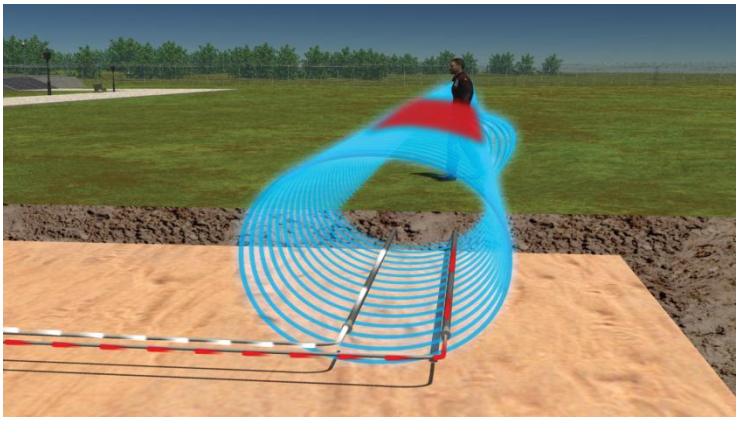
Buried cable sensors

This is a virtual fence implemented by a smart cable, buried less than one foot underground. The cable creates an invisible electromagnetic field, capable of detecting any intruder entering that narrow virtual corridor. This is not an inexpensive solution; however it is an ideal solution for places where a fence cannot be installed – be it due to aesthetic reasons or environmental concerns. The fact that it is a concealed detection sensor makes it unbeatable and ideal for protecting the internal quarters within an airport where a "fenceless" fence is desired.

Buried cable is also an ideal solution to protect aircraft parking areas and hangars, where the tarmac needs to be trenched for creating a virtual fence and where a real fence cannot be erected. Some of the solutions in the market can pinpoint the intruder along the corridor with a resolution of a few meters. This may be important taking into account that this virtual fence does not delay the intruder.

OmniTrax®

OmniTrax® is the fifth generation, covert outdoor perimeter security intrusion detection sensor that generates an invisible radar detection field around buried sensor cables. If an intruder disturbs the field, an alarm is declared and the location of the intrusion is determined. Targets are detected based on their conductivity, size and movement.



Cables can be buried into a variety of surfaces (ground, grass, concrete) approximately 23 cm (9 in.) below the surface and are completely covert. The cables are robust enough for direct burial in most surfaces. The terrain-following, volumetric detection field is typically 1 m (3.28 ft.) high by 3 m (9.84 ft.) wide by up to 800 m (2625 ft. or 1/2 mile) long per sensor processor. Systems can be

standalone or networked for long perimeters whereby sensor cables are connected together to create a continuous perimeter.

Microwaves

This sensor is another type of a virtual fence based on electromagnetic transmitters above the ground that create an invisible detection beam. Any intruder going through the field will disturb the beam and cause an alarm. Two types of microwaves are available: a) bi-static – composed of a transmitter on one side and a receiver on the other side. b) mono-static - where the same unit does both. A single pair of Bi-static microwaves can cover 100 to 300 meters.

The technology is easy to install but requires constant grass cutting. It is ideal for places that may be open to restricted traffic – be it on a temporary basis, where infrastructure construction is underway,
or for longer term. Like any other virtual fence, it misses the deterrence and delay function.

Smart CCTV

Outdoors cameras, equipped with outdoors Intelligent Video Analytics (IVA) are an excellent sensor to protect and complement every perimeter as well as the internal sections and infrastructure within the airport, especially if designed by outdoors experts with professional outdoors algorithms.

Integration

Airports security decision makers need to emphasize and recognize the importance of an integrated solution that marries everything into one coherent manageable system. All security systems depend on human intervention and therefore should be based on the overall reliable alarms, notification, and situation awareness. Due to the critical nature of any event in an airport, quick reaction and immediate response depends very much on the quality of the head end: the Command & Control center. Today's PSIM (Physical Security Information Management) applications are at the heart of any real-time decision process.

The PSIM connects and integrates all sensors and correlates multiple inputs (cameras, gate control, access control, PIDS sensors, etc.) as well as other applications into a single synchronized display. A Graphical Information Systems engine is used as a platform to arrange layers of data, ensuring accurate location and cross reference between the fielded sensors, the maps and the mobile forces.

µltraLink

Senstar's µltraLink Input / Output (I/O) modules are hardware components that form an integral part of Senstar's system integration capability. µltraLink I/O modules attach to Senstar's Silver Network and provide a range of I/O types including outputs (relay, open-collector), and supervised dry-contact inputs. µltraLink outputs can be used to transmit alarms from Senstar's family of networked sensors using only Senstar's Network Manager Service software (NMS). For more sophisticated applications µltraLink I/O modules can be controlled by Senstar's StarNeT™ 1000 or Alarm Integration Module (AIM) software.

Summary

Securing the world wide air traffic is a “game” where a full teamwork is required – intelligence, counter terror measures, airport authorities, airlines and many more. Security managers must chance their focus from increasing the perception of protection with highly visible screening measures, and focus on creating a complete and functional security solution.