

## Why airport PIDS?

### ***Why football teams cannot afford to compromise their goalkeeper?***



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.

Most of the airports, if they do have a full fence coverage, this is simply a ***dumb fence***, without any detection capability. So, surprisingly enough airports are investing billions on the obvious security measures we see as members of the travelling public – screening, cameras and sniffers; yet the main door and 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? Here is a true story. A man living near a main US hub was walking his dog outside the perimeter one day and somehow the dog managed to escape and climb the fence. The man, without any hesitation, followed his dog into the secured zone. This may be considered a minor security violation, yet the event can easily turn into a safety issue.

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.

### So, where do we begin?

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 following are some specific guidelines for building a robust and efficient solution.

### Protect your perimeter with a smart solution

Unless you can place a guard every 300 meters of your airport perimeter, technology is required. Dumb technology cannot do an effective job in totality:

- A **dumb fence** only partially does the job – it **deters** and **delays** intruders, yet it does not provide **detection capability**; if someone decides to climb or cut through the fence, the intrusion, if noticed at all, will not be addressed.
- **Dumb cameras** alone are almost useless; even with every inch of your perimeter covered by dumb cameras, it's not enough. Multiple cameras without **automatic triggering** of alarms typically provide post-mortem information, once footage is reviewed.
- A combined solution of a **dumb fence covered by dumb cameras** is also not enough; many security tests have demonstrated that it is not practical to monitor hundreds of cameras manually. Experiments show that security personnel, watching 9 (!) cameras, **lose alertness** in less than 10 minutes.



## A dumb fence with smart cameras

**Smart cameras** include the processing capability to **automatically analyze irregular events** within a video stream; for example – an intruder crossing a line or other IVA algorithms (Intelligent Video Analytics). Although this is a popular solution it suffers from some inherent limitations:

- If the only trigger for an alert is a CCD camera, **many fixed cameras are required** to enable complete coverage, typically every 60-90 meters. Megapixel technology can double the range of a single camera but still does not change the fundamentals.
- Installing many **cameras** to cover is **quite expensive**, especially considering the deployment cost of power and the wide band communication required for the video transmission.
- A good outdoor **VMD processor** (Video Motion Detection), which is the classic smart video algorithm for virtual fences, is not easy to find and is a fairly expensive solution. Unlike indoor VMDs, an **outdoor VMD** must meet the challenges of moving shadows and trees clouds, glare, rain, snow and it should perform under extreme changes in lighting conditions.
- Simple **long range PTZ cameras** cannot serve as a trigger for alarm, since they can only examine the perimeter randomly. There are a few sophisticated CCTV solutions based on long range cameras, but these are expensive and **vulnerable** to the inherent limitation of CCTV (see below).
- **CCTV** is inherently **limited in bad visibility conditions** – fog, rain, direct sun glare and therefore, typically lighting is required for night, which is expensive by itself. At night, as an example, the combination of snow and lighting can reduce the POD (Probability Of Detection) significantly, or alternatively, create many false alarms.
- **Thermal imaging** cameras may solve some of the lighting limitations, but they are expensive and still do not work under heavy fog conditions.

## 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 Int'l) choose four layers for better confidence.

Every site is unique and hence the solution; however here are a few technologies along with their strengths and weaknesses:

### Technology review

**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** (POD vs. FAR) with demonstrated high **POD (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 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. If, on the other hand, a new fence is being erected, the overall cost may be not too far from the cost of a taut wire solution. 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 vs 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.

**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, or as a **second invisible tier**.

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.

**Decorative Fence** – these are **innocent looking** fancy fences equipped with **internal sensors** that will detect climbing, bending or cutting. Typically the decorative fence is used for limited **lucrative areas** within the airport, mainly due to the cost of the basic fence.

**Massive smart bars** – these are massive physical grids with embedded intrusion detection sensor/s. Each one of them is typically tailored to the specific dimensions of the **pipe, drain, open tunnel, canal or air duct** that it is meant to protect. Several techniques are available to ensure consistent water flow and to overcome silt build-up which could block the grid. These locations are regularly below surface and unfortunately overlooked, thus can be considered as **weak spots** to take note of.

**Radar** – ground protection radars are becoming more popular as an **additional layer** in the overall PIDS solution. Radars must have **line of sight** / cannot be obscured by obstacles, so as a general statement airports are ideal for radars, as they are flat and generally open. True, radars cannot deter or delay an intruder, but in many cases it can supply an **early warning** and also **track the intruder** until successfully intercepted by first responders.

Radars have no value in areas of heavy traffic or populated quarters; once the object has intruded the airport and “mingles” with the airport employees it is not effective.

Radars usually cover a large area and as such if one fails the entire area may be without any security measure.

**Microwave ( $\mu$ W)** – 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  $\mu$ Ws 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  $\mu$ W 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.



**Other virtual fences** – The outdoor security market uses many types of virtual fences like: **Passive IR** detectors, **Active IR / laser beams**, scanning laser beams, etc. All of these may be sufficient for private applications but are rarely used for wide area and **long perimeter** protection. They are simply not **robust** enough for harsh weather conditions and can have too many false alarms.

**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 C&C (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. GIS engine (Graphical Information Systems) 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.

### 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 - just like in a football game (soccer in the US). ... **Your PIDS is your last defence – Would any football team compromise its goalkeeper?**