



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

**Securing Critical Infrastructure:
Perimeter protection strategy at key national security sites
including transport hubs, power facilities, prisons and
correctional centres**

**By: Jonathan Murray
November 2012**

Contents

Background	2
Concept of Operations (CONOPS)	3
Chemical Facility Anti-Terrorism Standards (CFATS)	3
D⁵ strategy	4
A balancing act	5
'No bad approaches, just bad applications'	6
How many technologies do you support?	6
How do you test your products?	6
Can we see references?	6

Background

The need for early warning of an attempt to breach a perimeter is hardly new. In 390BC it was the cackling of the sacred geese of Juno that alerted Romans to the fact that a Gallic army was scaling the city walls. Similarly, the merits of different perimeter protection methods have been a subject of debate for 2,000 years since the historian Livy (59BC – AD17) ridiculed Greek palisade fences for being porous compared with Roman equivalents during the Second Macedonian War.

What is really new on the contemporary scene is the resourcefulness and disregard for civilian casualties shown by those who would act against society. As a threat to physical security at infrastructure sites worldwide, terrorism currently heads up a list that includes anti-government protests of an intensity not seen since the 1960s, large-scale illegal border crossing and commodity theft.

While international sharing of intelligence continues to improve, physical security provision remains a local matter and one in which the perimeter will always be the first line of defence. Perimeter security can not only detect but defeat attacks on the facility it is protecting if management opts for appropriate products and usage methods. It is therefore crucial that clients should work with vendors who offer the widest possible range of technologies in order that equipment can be optimized for the specific needs of the site.

It is our experience that, all too often, limited resources mean the security community focuses only on the most recent catastrophe or near-miss rather than risk prevention. It is, of course, impossible to protect a whole seaboard but analysts of the 2008 attacks in Mumbai have noted that when 10 terrorists landed on the city's beach in inflatable speedboats, the only delay

they experienced was while telling some curious fishermen to ‘mind their own business.’

Concept of Operations (CONOPS)

Comprehensive security provision comprises three key elements: technology, human resources and processes. All are integrated and adhere to the site’s Concept of Operations (CONOPS). But even at high-risk sites with clearly-defined perimeters, it is sometimes impossible to predict the mode of assault. Thus, a Jeep Cherokee loaded with propane canisters being driven into the doors of Glasgow’s International Airport Terminal in June 2007 would hardly have seemed a credible type of attack to security managers. But this was how Scotland experienced its first terrorist incident since the 1988 Lockerbie airline bombing.

Rudimentary perimeter protection in the form of bollards prevented the vehicle from entering the Glasgow terminal building and the terrorists had ruled out an attack on the chain link with razor wire top external fences. Had they breached this perimeter they might have been able to blow up one of the airport’s fuel depots.

Federal prosecutors in New York have alleged that later in the same year, Islamist terrorists plotted to blow up fuel supply tanks at John F. Kennedy International Airport in an operation designed to “dwarf 9/11.” JFK seems to be rarely out of the news and in August 2012 a stranded jet skier abandoned his craft, climbed an eight-foot electronic fence and walked undetected across two runways and into a terminal building.

Mainstream US media were quick to name the security provider and quote the cost of the installation, noting that the \$100m system had been provided by Senstar’s competitor, Raytheon.

Chemical Facility Anti-Terrorism Standards (CFATS)

Many critical assets around the world need better protection and would benefit from a call to action from governments and industry watchdogs. One sector at least is being well served in the US where government concerns produced the **Chemical Facility Anti-Terrorism Standards (CFATS)** whose many **perimeter intrusion** recommendations include detailed advice on the increasing threat of fence attacks involving vehicles.

The list of critical infrastructure assets needing perimeter protection continues to grow. Most are targets for different reasons:

Pipelines and Oil & Gas facilities – the potential for catastrophic explosions, threatening lives and property, economic disaster caused by reduced production and availability of fuel

Transportation hubs – large gatherings of populations, where many lives can be impacted with little effort, controls the flow of goods

Water Utilities – disruption or sabotage of treatment and contamination of distribution can lead to mass illness and death

Power Utilities – disruption can cause massive economic, social and health issues

Communication Utilities – disruption can reduce effectiveness of security and protection measures, likely a starting point for multiple attacks to slow response times

The current focus on renewable energy has increased the profile of solar energy plants and put a media spotlight on major facilities such as the soon-to-be-completed \$375,000,000 Moura photovoltaic farm in eastern Portugal. Senstar has estimated that the likely cost of equipping, installing and commissioning its 3,000 metre perimeter with a terrain-following volumetric sensor using four parallel field and sense wires would be in the order of \$300,000 (\$125,000 materials, \$175,000 for installation).



Precise cost-benefit analysis is not possible but set-up costs for perimeter intrusion at new facilities should be evaluated in the light of recent massive power failures. Notable outages affected southern California in September 2011 and twenty-two states in India when a staggering 9% of the world's population was without power for two days in July 2012.

The US incident was the result of multiple discrete events and the cause of the Indian failure is not known though irresponsible overloading is suspected. Neither outage arose from breach of a perimeter but the knock-on costs of the incidents should be apparent to specifiers as they design the next generation of facilities. Senstar executives recently visited an electrical

transmission station in South Africa where the client's perimeter fence had been breached by digging. A trivial incident of metal theft netting a few hundred dollars resulted in direct damage through loss of grounding of more than \$20m.



D⁵ strategy

It has already been demonstrated that the essence of securing a perimeter has not changed in 2,000 years. The key elements are **demarcation, deter, detect, delay** and **defeat**.

The first two are givens: the perimeter should be demarcated visibly so that an intruder knows he is trespassing. A visual sign will hardly bother a real intruder but it can prevent innocent trespass. Thus, the case in 2009 of the American hikers who allegedly crossed into Iran while walking in Iraqi Kurdistan could have been prevented with simple signage. The absence of simple border signs led to the male hikers spending two years in prison and only being released after intervention by United Nations secretary general Ban Ki-moon and payment of \$465,000 'bail.'

Deterrence in the form of a high fence with sharp edges and possibly razor wire topping is a basic ingredient, and evidence that such a fence has been scaled will quickly establish hostile intent beyond dispute. Detection will usually occur through use of sensing devices in a fence or by video surveillance. Ideally, detection will be achieved before an external perimeter is breached or while the intruder is in a 'sterile zone' between first and second-tier fences.

Typically, delay will occur as an intruder struggles to cut or lift a fence or, at a site with multiple levels of perimeter security, as the intruder negotiates the 'sterile' zone. Such an area may offer additional potential for detection and pinpointing of the intrusion in the form of covert buried sensors with an invisible volumetric detection field, microwave sensors or even IR detectors. Defeat occurs when delay is sufficient to allow a guard or other first responder to intercept and restrain the intruder.

A balancing act

The key to successful perimeter intrusion strategy in which staff will be motivated to 'buy into' and 'own' the technology is balancing probability of detection (Pd) with a very low false alarm rate (FAR) and a good nuisance alarm rate (NAR). A nuisance alarm occurs when equipment is not at fault but exact calibration is difficult to achieve or simply impossible. Thus, buried sensors in a sterile zone calibrated to alert on human footfall but producing an alert under the weight of wildlife of a comparable size constitute an example of a nuisance alarm.

No security technology can operate in isolation from other disciplines. The core technology of a Perimeter Intrusion Detection System (PIDS) is likely to be one or more 'smart' fences (a fence with detection capability rather than a 'dumb' barrier) complemented by buried sensors and ideally networked into a central command and control center. It is a common mistake to build a security installation solely around cameras, a strategy which is only effective if the sole objective is to gain video footage of intrusions.

An appropriate ratio between Pd and FAR/NAR can only be achieved if cameras are used in conjunction with 'smart' fences. With their substantial perimeters, infrastructure sites usually demand that both fence and camera should be 'smart.' (By a 'smart camera' we understand one that is equipped with genuine video analytics based on artificial intelligence rather than crude motion detection.) 'Dumb' fences and cameras without analytics are insufficient. A fence that offers only a physical barrier and does not generate an alert when it is cut or scaled by an intruder is inappropriate for critical infrastructure usage.

By way of example, take a medium-sized infrastructure perimeter of eight kilometers. Even with the advent of high-definition (HD) or megapixel technology, it is likely that - depending on terrain - at least 80 cameras will be needed. Security personnel tasked with monitoring only nine cameras lose alertness after 10 minutes, a statistic which means that manpower at such a site would be overwhelmed by the need to view screens. Cameras capable of discriminating between atypical and ambient movement through intelligent scene analysis would be a prerequisite.

'No bad approaches, just bad applications'

Many security consultants will glibly (and untruthfully) tell you that there are no bad sensor methods, just bad applications and bad integrators. Any critical infrastructure site that is serious about optimizing its perimeter protection should strive for a composite solution that plugs all the gaps and is responsive to the unique demands of a location. It therefore makes sense to look for a manufacturer which covers all the main sensor technologies. These are:

Taut wire, a hybrid system of sensors woven into a barbed wire fence known to offer a high probability of detection and FAR/NAR of close to zero. It is expensive but ideal for critical infrastructure where detection, delay and deterrence are vital.

Fence-mounted sensors, a cost-effective addition to existing fences which should be used in conjunction with CCTV as a verification tool to optimize FAR/NAR.

Buried cable sensors, a virtual fence achieved by burying smart cables as little as nine inches underground. Ideal where aesthetic considerations preclude a fence, and capable of detecting any intruder entering the narrow virtual corridor. Accurate location rather than rough zoning of intruders is required since a virtual fence causes them no delay.

Microwave (μW), the electromagnetic beam creates a virtual fence that is ideal for virtual gates where the 'gate' must be open for traffic during peak times and shut out of hours. This can be used as a

stand-alone detection layer, often on top of a wall or on temporary constructions.

Ground protection radar is well-suited to the open, clear areas of a port where early warning can reduce a first responder's reaction time.

Choice of manufacturer

Rather than steering readers towards Senstar, we prefer to pose a few questions that might be asked of other vendors.

How many technologies do you support?

If the vendor has only one core technology then be prepared for specious arguments that dismiss all other approaches as ineffective. Choose a vendor who is agnostic as to approach.

How do you test your products?

Outdoor sensors must be tested rigorously (technically and operationally) in harsh conditions over long periods. They must withstand many years of unattended service in environments that can be extreme in their electromagnetic conditions and salt levels. Does the vendor have their own test site or do they use clients to mature their technologies?

Can we see references?

Reference sites need to be mature, have a high profile and be directly relevant to the proposed project.

How will the solution integrate?

Comprehensive solutions must have a demonstrable ability to integrate and adapt to changing environments. Ease of integration through dry contacts as well as flexible networking are key.