Focusing on the perimeter for
Critical Infrastructure Protection (CIP)

The threats

The 21st century brings with it a constant risk of **terrorist attacks**, large scale **illegal immigration**, increased **crime** and violent **anti-government** protests as a result of international and local issues; it is a small world and it is getting smaller every day.

The most cost effective way to address these challenges is through international sharing of **intelligence** and preemptive action against those that would act against civil society. However, early detection of hostile intent and prevention cannot be counted upon to always work, and individual critical infrastructure facilities must therefore have the physical means to both detect and defeat attacks when everything else fails. In **physical security**, the perimeter is the first line of defense.

Priorities

It is clearly impractical to protect everything and attempting to do so with limited resources would simply result a low level of protection for everything. While security priorities are typically defined locally there are still common threats worldwide. The highest priorities are critical national assets where terrorists can, with a little effort, create massive damage and impact. Among these we see: **airports**, with a Sept. 11th or a KLM Lockerby scenario in mind; **seaports** and **sea shores** with a Mumbai offense in mind and even more catastrophic, the possibility of a **dirty bomb** being smuggled into a large city. **Nuclear stations** are seen as an even greater risk after recent events in Fukushima crisis; and finally; major international **sporting events** provide a perfect stage for opportunistic terrorists to "make their mark".

Unfortunately the security community is all too often trying to cope with the last catastrophe, rather than trying to **prevent the risk**. For instance, many senior security experts suspect that the high investment in passengers screening has simply pushed the enemy to look for the next weakest link in the security chain, the **unprotected airport perimeters**.

But there are many other critical assets around the world that need better protection; including: **chemical sites**, now being regulated in the US under the **CFATS** initiative (Chemical Facility Anti-Terrorism Standards); **prisons** in Mexico, where organized crime is direct threat to civil society, **oil and gas** facilities upon which the world economy relies; **military sites** and **borders** in areas of tension like Korea and the Middle East. There is also a requirement to protect against **Illegal immigration** like from Africa into Europe and a real need protect against theft from **pipelines** which is a daily occurrence in countries like Mexico and Nigeria and which can lead to tragedies like that which happened December 19th in San Martin, Mexico, where a pipeline explosion killed about 30 people and injured 50 more.

The list of critical commercial assets needing protection is also getting longer and longer. Examples include **solar farms** in Europe or an **electrical substation** in South Africa, where the soaring price of copper has made a grounding cable attractive target for thieves and resulted in millions of dollars of direct damage as well loss of essential electrical services.

D^5 strategy

The essence of securing the perimeter hasn't changed since ancient times – **D^5 – Demarcation, Deter, Detect, Delay and Defeat the intruder**.

The first two "D"s are very basic: the perimeter should visibly be *demarcated* so that an intruder knows he is trespassing! Adding *deterrence*, be it by sharp edges or high barriers discourages attack and makes determining hostile intent even easier, as intruders who make the effort to cross the barrier are more likely to be hostile!

The last 3 Ds complete the strategy; an intruder has to be reliably *detected* (3rd "D") as soon as possible, but not before actually breaching the perimeter. Then, once detected, he/she has to be *delayed* (4th "D") long enough to enable deploy the guard force to intercept and *defeat* (5th "D") the threat.

Advanced detection technologies

Industry has developed sophisticated sensors to ensure detection of intruders with a very high **probability of detection (Pd)**, a very low **false alarm rate (FAR)** and a good **nuisance alarm rate (NAR)** even in demanding outdoor conditions.

Need for Smart, Integrated Security Solutions

Comprehensive security is comprised of three key elements: **technology**, **human resources** and **processes**, all integrated and working together and adhering to the **CONOPS** – Concept Of Operations.

The core technology of the **PIDS** (Perimeter Intrusion Detection System) includes **smart fences** and **gates**, ideally **networked** into a central **command and control center**.

Verification and surveillance cameras to manage FAR/NAR are also an important element of any full security solution; however many first time security players fall into the trap of building their concept only around cameras which is only effective if you define your security objective as recording rather than detecting and preventing security incidents. Cameras (basic or smart) without smart fences are simply unable to deliver the appropriate ratio between the Pd and FAR/NAR.

Ineffective PIDS strategies for CIP

Basic Fences Only without detection technology demark and deter intruders but can easily be *cut or climbed* without being noticed; especially in large sites that host critical infrastructure.

Basic Fences and Simple Cameras - a combined solution of basic fences covered by simple cameras is also inadequate. By way of example: a medium size site with 8Km long perimeter would require 80 to 150 cameras (depending on resolution) to effectively monitor intruders. It is absolutely not feasible to manually monitor such a large number of cameras. In fact, studies have shown that security personnel tasked with monitoring only nine cameras *lose alertness* in ten minutes; CCTCV effectiveness drops significantly in *low visibility* like at *night*, in *fog* or in *heavy snow*.

Basic Fences and Smart Cameras can automatically analyze **irregular events**, however a combination of a simple fence with smart cameras will not provide an efficient security; it is quite an expensive solution: many static smart cameras, **illumination** for night time, **IVA** optimized for **outdoors** and a lot of investment in **infrastructure** (power, bandwidth, storage); but still without solving the inherent CCTV limitation – poor to no performance in fog, snow and heavy rain conditions.

Thermal imaging cameras with intelligent **video analytics** (IVA) may mitigate some of the limitation but they are expensive and are more suited to a role of a complementary sensor for **verification and tracking**, once the intruder has been detected by another sensor.

Optimum PIDS strategies for CIP

Multi layer system - the more critical sites require *multi layer PIDS*. The perfect example is nuclear sites; they always have two layers of fences with typically 2-3 detection layers. A very common architecture is an initial layer of a tall volumetric sensor (4-6 meters high!) with a very high Pd. Once an alert is generated, the intruder has to penetrate a barrier and which even if the intruder is well equipped, should take a few minutes to move on. The next space is a *clear zone*, typically of about 10 meters wide; it is an area always kept clear, facilitating ease of verification, be it by cameras or another layer of PIDS, such as *microwave sensors*, *buried volumetric cable* or even *IR detectors*. And finally there is typically a second barrier for further delay and sometimes another layer of detection.

Multi sensor systems – every detection system has some *limitations* and every site has *unique requirement* and constrains. Therefore a good solution should consist of a mix of complementary sensor technologies, each tailored to the specific case, in order to provide *complete coverage* without gaps. Many high security projects use *hybrid solutions*; but such organizations are often reluctant to publically disclose their protection strategy. An example of an advertized site is the *New Delhi* International Airport (IGA), where they have implemented a mix of *four layers* / types of sensors: an outer layer of *taut wire*, a *buried cable* as an inner concealed layer, *surveillance* cameras for verification and tracking and several *radars* for early warning and uninterrupted all weather tracking.

Which PIDS technology is the best?

Many security experts would tell you that there are no bad sensors, just bad applications (and sometimes bad installers). Finding a **knowledgeable consultant**, system integrator and/or **PIDS supplier** with verifiable **PIDS references** and access to a wide array of PIDS technologies is probably your best insurance for obtaining the desired result. Nevertheless here are the main sensor technologies that are commercially available.

- **Taut wire** – A hybrid system of sensors weaved into a **barbed wire** fence. This fence offers **guaranteed performance** in all-weather conditions. It has demonstrated a high probability of detection (POD) and an almost **zero FAR/NAR**. It is not cheap but ideal for high security, where deterrence and delay must be achieved on top of **uncompromised detection**.

- **Fence-mounted sensors** – These sensors are ideal add-ons to existing fences as an affordable solution. A second security measure, such as CCTV, is recommended as a verification tool to manage FAR/NAR.

- **Buried cable sensors** – A **virtual fence** implemented by a smart cables, buried less than 9 inches underground. These cables create an **invisible** electromagnetic field, capable of detecting any intruder entering the narrow virtual corridor. The buried cable sensor is an ideal solution for places where a fence cannot be installed for **aesthetic or environmental** reasons, such as concrete platforms where movement must be enabled only during active parts of the day. As a concealed, terrain following sensor It is almost **unbeaten by intruders**; therefore in many places it is used as a second layer – sometimes outside of a fence but more commonly as an inner detection layer. Since virtual fences do delay the intruder, accurate **location (ranging)** of an intruders (rather than rough zoning) is essential to enable the effective intercept of intruders.

- **Microwave** (µW) – Another type of **virtual fence** that creates an invisible electromagnetic beam. This is ideal for **virtual gates**, where the "gate" must be open for traffic during the daytime but must be shut down at off-times, such as nights or weekends. It is also used as a standalone detection layer – either on **top of walls** or **dead zones** in prisons but also for temporary constructions, when the "virtual gate" must be easily installed and removed later.

- **Tailored robust grids** – these are designed to plug critical holes in perimeter security systems by custom fitting a specific opening, such as **canals, pipes, open tunnels or drains**. The grid is fortified with either electro mechanical or electro optical sensors threaded within the steel.

- **Radar** – Ground protection radars are ideal for a port's open and clear areas (i.e. no traffic), where early warning can significantly reduce the first responders' reaction time.

Which vendor should be chosen?

Rather than answering this question, here are a few questions to ask your potential vendor:

- **How many technologies do you support?** if the vendor has only one core technology, you better be careful, because no matter who you are or what you need – you will end with one option plus tons arguments proving that all other technologies are useless. Choose a vendor that cares for the customer but is agnostic to the preferred technology. The more *variety* of supported technologies, the more you can choose from.

- **How do you test your technology?** outdoors sensors must be tested rigorously - technically and operationally in harsh weather, over long periods, and withstand many years of *unattended service* in *salty* climates, in tough *electromagnetic environment*, etc. Does the vendor have their own *test site* or do they use their clients to mature their technology?

- **Show me your references!** and they better be of high security profile, in similar places, various vertical markets, and most importantly – that are working for many years for as many as possible happy customers.

- **How well will your solution integrate?** a full *comprehensive solution* must be *integrated* and should be able to grow and adapt to *changing requirements*; therefore *ease of integration* through dry contacts as well as flexible networking is key, even if you start small and basic.