A Senstar Inc. White Paper

13800 Coppermine Road
Herndon, VA 20171
703.463.3088
www.senstar.com

Life on the Edge:

Securing the Perimeter with respect to CFATS (Chemical Facility Anti-Terrorism Standards)

By: Kenneth Ribler
Executive Director Government,
Commercial & Emerging Markets

September 12, 2011

Contents

The threats

Threats and risks to our communities, rural and urban alike, have created the demand for keen attention to the criticality of securing Chemical and Petroleum facilities located in these communities or communities located in close proximity to them. From basic criminal activity to terrorism (domestic, international or transnational), these threats warrant a focused level of attention and action to ensure the public remains safe and these industries remain secure.

The 2007 establishment of Department of Homeland Security (DHS) regulations serves to regulate security practices at facilities that DHS determines as "high risk" according to the National Petrochemical & Refiners Association and is based on:

- potentially severe consequences
- the health and safety of citizens in the area
- national economic impacts

Attacks on petrochemical storage sites, manufacturing locations or distribution points can range from simple threats such as small arms fire or small quantities of explosives directed at these locations, to complex and highly elaborate and precise targeting of select critical assets or manufacturing processes with the intent of causing catastrophic damage or loss of life . In either scenario, the distinct possibility of massive amounts of damage to the facility exists resulting in potentially staggering levels of loss of life or injury to workers and the general public if these chemicals are released into the atmosphere or water systems. Equally unsettling is the specific targeting of the riskiest and most dangerous chemicals for theft or diversion for the purpose of terrorist actions against other critical infrastructure locations or population centers. The ability of terrorist groups to further weaponize these chemicals by combining them with explosives exponentially increases the

lethality and broadens the possible impact plumes as a result of detonation. The economic consequences associated with these actions are devastating at both a national and international level.

Background

Critical to the discussion of standards and the implementation of effective security solutions (in terms of policy, integrated systems and effective training) is that CFATS compliance will only happen through partnerships and collaboration amongst all stakeholders. Effectively, DHS, the chemical companies, perimeter security companies, system integrators and guard force personnel agencies must work together to develop viable solutions to counter any potential terrorist attack that could lead to the release of the 325 "Chemicals of Interest" identified by DHS. Even their theft or sabotage poses a high risk factor and maximizing our resistance to those threats is critical. The obvious challenges of assuring the protection and overall security of these facilities and storage locations are exacerbated by the fact that they are everywhere, throughout the United States and around the world. It will only be a matter of time when other nations will be employing similar levels of CFATS regulations. [Note: Though CFATS standards are specific to Chemical industries, the inclusion of Petroleum industries in the overall discussion of risk based solutions is instructive in addressing threats to facilities/assets.]

According to a Security Management article "*CFATS and Comprehensive Chemical Security Management*"(by Lee Salamone, Brad Fuller, and H.M. Leith), almost 36,000 sites that possessed the listed Chemicals of Interest (COI) were required by the CFATS regulation to complete screening assessments to determine relative risk, based on security vulnerabilities. Facilities identified as being the highest at risk were then required to complete a Security Vulnerability Assessment (SVA). A staggering 7,000 separate locations originally fell into this category of being at the highest risk level. Though these locations have been reduced to almost 4,600 (mainly due to COI removal and quantity reductions), these facilities are literally in the "backyards" of thousands of highly populated communities.

Though there are still many unanswered questions regarding the establishment of specific standards and objective measures for security system installation, it is apparent that to protect these facilities and the communities that surround them, a status quo approach is clearly unacceptable.

To their credit, DHS has helped establish Risk-Based Performance Standards (RBPS) for the industry, and companies are now required to address their approach in protecting their assets in their respective Site Security Plans.

Need for smart, integrated security solutions

What remains to be done?
It's a five prong approach:

1. Commitments from the chemical industry and system integrators to develop the most cost effective and scalable solutions to address the vast array of security challenges, unique to each location and to individual environments in which they reside.
2. The use of industry leading technologies to deter, detect, delay, assess and respond, to effectively manage the risk, is paramount.

3. Recognition and acceptance that a "one size does not fit all" strategy will help devise a solution that fits the application – appreciation of the sheer complexity and magnitude of establishing effective countermeasures against terrorist threats should be obvious.
4. A layered approach is the answer – The ASIS International Facilities Physical Security *Measures Guideline* approved in June 2009, identifies the criticality of defending against illegitimate and unauthorized activities at the perimeter (or "outer layer" as addressed in their concept of *Layers of Security*).
5. Deployment of a reasoned and rational integration of systems that capitalize on the basic, but sound principles of assuring high probabilities of detection, and very low nuisance alarm rates has been proven to be effective and the most cherished fundamentals when architecting an integrated security solution.

In the article, *CFATS and Comprehensive Chemical Security Management,* the issue is summarized in a way that succinctly defines what needs to be done:

"Since many facilities will require security upgrades to meet the RBPS, it is crucial that the investment in security systems, equipment, and layers of protection meet the needs of DHS as well as the full range of critical assets, threats, and vulnerabilities that a security manager needs to understand and address".

Comprehensive security is comprised of three key elements: technology, human resources and processes, all integrated and working together.

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 are also an important element of the full solution. Many security players fall into the trap and build their concept around cameras rather than alarming detectors; as explained below, cameras (basic or smart) without smart fences will simply not deliver the appropriate ratio between the Probability of detection (Pd) and False Alarm Rate (FAR).

What PIDS would not work for petrochemical protection?

Basic Fences Only - simple fences without detection technology demark and deter intruders but can easily be cut or climbed and going unnoticed; 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. Consider this: A medium size site with 8Km long perimeter would require possibly 80 to 150 cameras (pending resolution) to monitor intruders effectively. 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 less than ten minutes! *And how about night time? And fog? And heavy snow conditions?*

Basic Fences and Smart Cameras - although smart cameras can automatically analyze irregular events, a combination of a simple fence with smart cameras will not provide adequate security due to a number of inherent limitations. In short, it is quite an expensive solution: multiple

static smart cameras, illumination for night time, intelligent video analytics optimized for the outdoors and a lot of investment in infrastructure (power, bandwidth, storage). This solution doesn't solve the inherent CCTV limitation – poor performance in fog, snow and heavy rain conditions. Thermal imaging cameras may address some of the limitations mentioned above but they are expensive and more fitted to a role of a complementary sensor for verification and tracking, once the intruder has been detected by another sensor.

What PIDS would work for petrochemical facilities?

Multi layer system - the more critical sites require multi layer PIDS. The perfect example is nuclear sites and select chemical facilities; they often have two layers of fences with typically 2-3 detection layers. Here is a very common architecture: 1st layer of a very high volumetric sensor (4-6 meters high!) with a very high POD. Once an alert is generated, the clock is ticking. Now the intruder has to penetrate a barrier / fence; even if the intruder is well equipped, it 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. The addition of a second barrier for further delay and sometimes with another layer of detection significantly enhances overall site protection.

Multi sensor systems – every detection system has its limitations. Every site has its own requirement and limitation. Therefore a decent solution should consist of a mix of technologies, tailored to the specific case, in order to provide coverage for the gaps – be it due to physical limitations (like a creek going through a fence), weather conditions or operational concerns (e.g. access limitation by the dispatched guards). Many high security projects will need a hybrid solution.

Unfortunately, when it comes to designing the ideal system to protect a critical site, organizations are reluctant to expose their story in public, making it difficult to educate those requiring such a system on the options available and how to deploy them. However, the New Delhi International Airport (IGA) security project is of public record. The customer has implemented a multi-layered approach with the implementation of four types of sensors: an outer layer of taut wire, 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?

According to the DHS CFATS Risk Based Performance Standards (2009), a well-secured perimeter will help deter intruders from trying to gain access to the facility or from launching attacks from the area immediately outside a facility's perimeter. These standards also stipulate that "there are limitless possible configurations of PIDS components that together satisfy the RBPS for securing and monitoring the facility perimeter. *The expectation is that owners/operators will implement and configure a set of security countermeasure components that will meet or exceed the expectations of the RBPSs for the tier-level metric that is applicable to their facility.*

By definition, there is no clear answer on what constitutes the "best technology." The combination of technologies has to fit the threat, operational concept, environment and budget. Here are the technologies available:

Fence-mounted sensors – These sensors are ideal for application to existing fences as an affordable and cost-effective solution. They provide the ability to detect cutting, climbing or lifting of the fence fabric at the outset. A second security measure that complements fence sensors is CCTV, which must be integrated as a verification tool of the initial detection technology, for high security sites.

Buried cable sensors – A virtual fence created by a smart cable, buried about 23 cm (9 inches) underground. The cable creates an invisible electromagnetic field, capable of detecting any intruder entering the narrow virtual corridor (2 – 3 meters wide) along the cable. The buried cable sensor is an ideal solution for places where a fence cannot be installed for operational, aesthetic or environmental reasons, such as concrete platforms where movement must be restricted during non-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 of the solution, sometimes outside a fence, but is more commonly used as an inner detection layer.

Taut wire – A hybrid system of sensors weaved into a barbed wire fence. This fence offers guaranteed performance in all-weather conditions. It has a very high Probability of detection (Pd) and an almost zero False Alarm Rate (FAR). It is more expensive than many solutions, but ideal for high security, where deterrence and delay must be achieved on top of uncompromised intrusion detection.

Microwave – 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, fences or for temporary constructions, when the "virtual gate" must be easily installed and removed later.

Tailored robust sensor 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.

Terrain-following volumetric sensors - These sensors create an electrostatic field around a set of parallel sensor wires that causes an alarm when intruders attempt to penetrate them. These systems can be free standing or fence/roof/wall mounted. The well-contained detection zone allows the sensor to be installed in a wide variety of applications with greatly reduced nuisance alarms. Mounting electrostatic sensors on existing fences can be an economical alternative to replacing or upgrading less than ideal fences.

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

Choosing a vendor

Rather than answering this question, here are a few questions to ask your potential PIDS solution provider / integrator:

How many technologies do you support?

If the vendor has only one core technology, you better be careful, because regardless of who you are or what you need – you will be left with one PIDS security option along with a plethora of arguments proving that all other technologies are

useless. Choose a vendor that cares for the customer but is agnostic to the preferred technology. The greater the variety of supported technologies, the more you can choose from and be assured you will have the right sensor for the right application.

How do you test your technology?
Outdoor 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 environments, etc.

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.

Show me your references!
Not to be trivialized, reputation and commitment to support the end-user cannot be overstated. Experience in similar high security profile configurations in various vertical markets is critically important.

Final thoughts

Stopping or deterring hostile intent at the perimeter or "on the edge" is a dominant and well accepted practice in traditional as well as future integrated security solutions. In the world of asset and personnel protection, keeping the adversary far removed from your area of interest and their area of influence (in terms of their destructive capacity) is what security plans, practices and security systems/technology are based on. The effective use of outdoor (edge) smart perimeter systems, installed as a standalone system or integrated into a larger set of systems, ensures that “Life on the Edge” can be a safe, secure and a value-added approach to countering terrorism and protecting this nation’s petrochemical industry and communities alike.

Author Biography

Kenneth Ribler is Senstar Inc.’s Executive Director of Government, Commercial and Emerging Markets based in Washington. He is an experienced security professional in the areas of force protection, anti-terrorism and law enforcement having worked as Director of Operations for L-3 Communications and Deputy Director of the Electronic Systems Squadron at Hanscom Air Force Base. Mr. Ribler also served overseas as the Director of Security, Headquarters 7th Air Force in Korea. He is a Certified Protection Professional (CPP) with ASIS International and serves as both their Co-Vice Chair for the Military Liaison Council as well as a member of the Critical Infrastructure Working Group.