

An insight into issues to consider when implementing protective measures for chemicals of interest (COI) in storage tanks or tank farms

Physical security considerations for CFATS regulated tank farms

Many CFATS regulated facilities manufacturing or storing chemicals in tank farms might be attractive to terrorists. Most of these facilities have submitted security vulnerability assessments (SVA), site security plans (SSP) or alternate security programmes (ASP) to the Department of Homeland Security and are awaiting notification of their final tier assignment. Regulated facilities must strive to achieve an approved SSPs which may not occur on the first submission.

The physical security expectations for CFATS regulated facilities can be found in a document entitled the Risk-Based Performance Standards (RBPS) published in May 2009. It contains 18 standards that apply in whole or in part to regulated facilities dependent on the type of COI and associated risk of criminal or terrorist attack. In the guide, risk-based performance standards one through four cover the bulk of the physical security expectations that will result in the majority of expense for regulated facilities. Therefore, it is essential to take a disciplined engineering approach to implementing measures to detect and prevent attacks to avoid unnecessary cost or inadequate systems that would be rejected by Homeland Security.

On some occasions, when an initial SSP submission is rejected, Homeland Security prescribes a Site Assistance Visit (SAV). When a SAV is ordered it usually means there are significant gaps in an SSP submission (e.g. complete sections of risk-based performance standards are omitted) and DHS believes they need on-site, face-to-face contact to resolve discrepancies.

A SAV is intended to inform site owners and operators about



Outrigger installed incorrectly

security vulnerabilities and gaps as well as protective measures to increase preparedness for all hazards, including terrorist attacks. This can be time-consuming and, in the case of a subpar SSP submission, is better avoided. It is one thing to ask for help, it is another to have it imposed on you. Homeland Security representatives will come onto your site, review your conditions, your site security plan and discuss potential options for closing gaps in your SSP submittal. This is guidance only and is not prescriptive. Representatives will not dictate solutions, nor make any representations that one measure or another will assure SSP approval.

Sites in this predicament typically have a fixed number of days to agree on corrective measures and resubmit an SSP, or are at risk of non-compliance. While we have not yet seen it exercised, the regulation does allow for fines up to \$25,000 (€19,000) per day for non-compliance.

As of October 2010, there were very few approved SSPs. However, eventually all facilities

will cross the threshold of having an approved SSP and will be expected to execute planned improvements to meet the appropriate standards. For tank farm operators this means preparing to defend against terrorist adversaries on foot or in vehicles. The information in this article is useful for operators that are still in the process of preparing their initial SSP submission, or for those who may be in the process of resubmitting a rejected SSP.

There are limitless possible configurations of intrusion detection systems (IDS) components that together satisfy the RBPS for securing and monitoring the facility perimeter. Buyers are cautioned to exercise due diligence in the development of compliance proposals to Homeland Security. Vendors are going to promote the merits of their own products, in some cases at the expense of looking at all potential solution sets. An independent security designer with experience in perimeter intrusion detection and anti-vehicle measures can best assist in sorting through the myriad of solutions

with objectivity and with no financial relationship with one manufacturer or another. In the US the International Association of Professional Security Consultants (www.IAPSC.org) and in the UK, the Association of Security Consultants (www.securityconsultants.org.uk) are two such organisations that can provide independent expertise.

Protection against attackers on foot

The target outcome is delay, early detection of an adversary, assessment to confirm the threat and response by adequate law enforcement or government agencies. If an adversary can complete their mission before interdiction by law enforcement agents, the programme cannot achieve success. In some locations this can present significant challenges suggesting the need for more robust delay measures.

To achieve delay, common anti-personnel barriers include fencing that is intended to deter and delay unauthorised access to a restricted access perimeter. The industrial consensus for

standard fencing is a 9-gauge chain link, 6-7 feet in height with a 1 foot top guard outrigger oriented in the direction of the threat. Very often this measure is seen installed in the wrong direction, in which case it serves as an aid to adversaries rather than a delay measure.

In instances where additional delay is necessary, high security fencing such as a welded mesh fence is effective as it is much more difficult to scale or cut through. Pricing for anti-personnel measures described here generally range from \$30 for a standard fence to \$80 for a linear foot, or more for a high security fence, depending on other amenities added to the barrier (e.g. concrete base).

To achieve early detection a site may consider any number of common detection technologies. During the last 25 years the application and sophistication of perimeter sensing technologies has grown tremendously. There is also a wide range of sensing technology types and installation methodologies (e.g. fence-mounted, buried, volumetric, passive infrared or microwave motion sensing, capacitance change sensing, seismic or vibration sensing) available for perimeter security that have remained stable during this growth period.

The most recent development, video motion detection and video analytics, has significantly advanced the application's ability to track, assess and localise an intrusion source for situation assessment, monitoring and response.

Essentially, perimeter sensing technologies vary greatly in their effectiveness, affordability, and accuracy. A recent project with a perimeter length of 1800' used video motion detection. The site featured extremely low light levels (the worst-case scenario). The cost of implementation for video detection was approximately \$90 per foot for low light cameras coupled with infrared illuminators and analytics. Note, however, that for tank farms that may be located inside of busy facilities with nighttime vehicle traffic, headlights passing through the field of view of video analytics relying upon infrared illumination will generate false alarms.

Where headlight incursion is possible, the other feasible option with little or no light is the use of thermal imaging cameras. Thermal imaging uses the natural heat signature of every object to form the image and it works in any lighting condition including the absence of light. These cameras are highly immune to snow, rain, fog and smoke, as they 'see through' those impairments. Because objects radiate their heat signatures differently and most are at varying temperatures to each other, these differences are easily discernable, and detection easily obtained. A thermal imaging solution for the 1800' perimeter case study above costs approximately \$125 per linear foot. Typically, the design basis for these types of detection solutions is based on the

detection of an adversary and not identification. This helps to keep costs down.

The next step is determining the means by which alarms will be assessed. In the scenarios above, two pan, tilt and zoom PTZ cameras were included for assessment of an alarm event by control room operators. Depending on the infrastructure available, images from closed circuit television CCTV cameras can be viewed locally or remotely in response to an alarm to evaluate the cause and inform law enforcement or security responders. Alternatively, personnel can be sent out to investigate alarms, but this sometimes raises issues of training or ethical issues of whether employees should be dispatched to a potentially dangerous situation, thus making the CCTV a lower risk assessment option. While other types of detection sensors can be installed for less, the assessment function needs to be considered for a complete programme. For example, fence mounted sensors could be mounted for less cost than video detection measures (e.g. \$40 per foot for a 900' perimeter), but those savings were offset by the need to run fiber for CCTV assessment cameras. There is no magic formula for what combination of technology and manpower will provide the most efficient and cost-effective results, but there is no doubt that a qualified security designer is essential.

Finally, a relationship with outside law enforcement agencies who will respond to the site and potential intrusions is necessary to determine response time and to conduct drills and exercises that validate response assumptions. Ensuring effective detection, sufficient delay through barriers, and efficient response are top priorities in the protection of tank farms against adversaries on foot. A useful reference in addition to the RBPS guideline is the US Army on Physical Security, entitled FM 3-19.30, specifically Chapter 6.

Protection against vehicle attacks

Storage tanks may also need to be protected against vehicle-borne improvised explosive devices. In these scenarios, vehicles would be parked outside or introduced into the tank storage area

by force. Sites will need to evaluate the extent to which adversary vehicles could be parked near a COI and also will have to prevent unauthorised vehicles from getting too close.

To this end, many tank farms have safety mitigation in the form of spill containment berms that are in place to assist in keeping unauthorised vehicles away from or out of the tank farm. These safety measures can be leveraged to meet security objectives, often with little modification to their current shape and height. The US Department of Defense has published design for anti-vehicle earthen berms. The idea of this configuration is that the adversary's vehicle would either be unable to scale the berm or would get stuck at the top and be unable to get within an unacceptable distance where an explosive could be detonated.

In cases where the earthen berm is used to funnel authorised vehicles to specific entry points, these maintenance entry points should be equipped with an anti-vehicle barrier such as a drop arm gate or other Department of State approved anti-vehicle barriers. This will ensure a complete anti-vehicle perimeter around the tank farm. Note that anti-vehicle barriers should be placed outside anti-personnel barriers, which are not typically resistant to vehicles. Sites need to avoid anti-personnel barriers being compromised by vehicles that intend to create unauthorised access on foot.

In summary, it is typically easier to protect a tank farm against a vehicle attack versus an attack on foot. Facilities must consider a number of environmental conditions when designing a perimeter intrusion detection system to protect a restricted area perimeter. The fundamental principles of detection, delay, assessment and response must be applied correctly in order to achieve system effectiveness. An investment in outside expertise to navigate CFATS compliance can reduce implementation costs and expedite SSP plan approval as well as avoid costly non-compliance fines. ●

For more information:

This article was written by Frank Pisciotta, president of Business Protection Specialists, an international security consulting firm, www.securingspeople.com

Adversary task time vs PPS time requirements

