

# Securing Oil and Gas Assets

a report by

**Yahya Mehdizadeh**

Surveillance and Security Division, SAIC

Oil and gas assets are under attack. For domestic and international oil companies, securing oil and gas assets has become imperative, as the nature of these assets makes them a target for malicious activities. Potentially, an attack could result in financial and environmental devastation, wreaking havoc on global economies, international trade and domestic necessities such as food distribution, emergency services and daily commerce.

Before finding a solution, it is important to understand the problem. Knowing what challenges are facing the industry, why these assets are under attack and what makes them vulnerable is imperative in order to be able to provide mitigation strategies based on physical security solutions. The concept of 'defence in depth' is used to present technologies that can reduce and manage risk levels, while the integrated approach focuses on command and control (C2) technologies that provide a holistic view to the security issues surrounding an energy asset.

This article does not endorse or recommend specific types of deterrent technology, but rather presents options to help understand potential security solutions.

## Industry Outlook

In 2007, the rate of oil consumption was 84 million barrels per day (bbl/d) worldwide. With an average annual growth rate of 3.8%, the International Energy Outlook (IEO) predicts that by 2015 consumption rates will increase to 98 million bbl/d and they will rise to 118 million bbl/d by 2030. With no significant slowing in sight, a recent benchmark index noted that over the past two years there has been a 53% increase in the cost of major oil and gas production projects.

## Vulnerability Factors

International terrorists are now attacking oil and gas installations. Factors making these installations susceptible to attack are their remote geographical locations, poor transportation and communication infrastructures, potential for capital for investment, geopolitical turmoil and production outputs. A 2006 study conducted by New York University's Wagner Graduate School of Public Service found that terrorists most commonly targeted production (15%) and distribution (70%) facilities; within the distribution facilities, pipelines are the most commonly attacked components.

Yahya Mehdizadeh works in the Surveillance and Security Division at SAIC, providing physical security solutions for high-value energy assets. He has over 18 years of experience in the oil and gas industry, designing and deploying information technology and security solutions for upstream and downstream businesses. He has had numerous articles published on security-related topics and holds multiple industry certifications in this domain.

## Assets Under Attack

Oil and gas assets are being attacked from all angles: air, land and sea. Offshore platforms, transport tankers, floating production, storage and offloading (FPSO) vessels and liquid natural gas (LNG) processing plants are the industry's most vulnerable assets. Intruders are leading paramilitary-style attacks using various attack vehicles, including boats, submarines and/or air strikes. Coastal-based refineries and ship channels are being targeted for underwater attacks. Land-based pipelines and refineries are the most vulnerable and frequently targeted installations.

Unauthorised perimeter penetration is the major physical security issue concerning refineries. Explosive projectiles launched from movable artillery are the most severe air-based threat. Direct air assault is a possibility, but its probability is minimised by national air space protection regulations.

## Mitigation Strategies

Detective controls such as surveillance, monitoring and intrusion detection are used to discover attacks. Once threat vectors have been identified, mitigation strategies are implemented to off-set these risks, triggering preventative or corrective controls that respond to and contain the assault.

Mitigation strategies are part of the overall security objective based on the defence in depth approach, in which multiple layers of protection are placed within systems, people, technology and processes. Each specific asset or location has its own unique factors that are considered when developing mitigation strategies. Preventative controls protect vulnerabilities, making an attack unsuccessful or reducing its impact. Corrective controls such as physical security and perimeter access reduce the effects of an attack.

Mitigation strategies begin with a comprehensive risk assessment, allowing for proper evaluation of the physical security of the energy assets. The assessment identifies what assets need to be protected and determines how critical each asset is, examining the impact of each asset as it relates to human resources, infrastructure and production. During the assessment process, threats and vulnerabilities are identified, characterising potentially hostile occurrences that directly affect the asset and could be capable of damaging others.

After completing the assessment, the next step is implementing the appropriate countermeasure. Countermeasures are deterrent in nature and reduce the likelihood of a deliberate attack, including perimeter intrusion detection and surveillance systems. Proper incident responses, policies, procedures and change management procedures are then put into place; these contain and manage risk levels, implementing control mechanisms such as authentication and authorisation systems and personnel security and awareness training.

### Physical Security Solutions

When securing maritime and land-based installations, early detection is the first line of defence to prevent unwanted attacks. Basing security on the principle of detect, deter, delay, defend and defuse, there are two strategies that prevail:

- hardening – preventing or minimising attacks by placing obstacles (walls, fences, cement barricades and fireproof gates) in the way of potential attackers; and
- systems deployment – breaches in security can be monitored and managed by deploying surveillance and notification systems such as cameras, motion sensors, lighting, heat sensors, smoke detectors, intrusion detectors, radar systems and alarms.

For oil and gas assets operating in hostile environments, long-range acoustic devices (LRADs) are known technologies that provide highly directional acoustic arrays designed for extended-range communication, warning and deterrence. Microwave deterrent beams are another device that can be utilised. These produce an intense burning sensation that stops when the transmitter is switched off or when the individual moves out of the beam. Effective lighting can also be an important part of a security strategy. Illumination provided by proper lighting increases the sensitivity of intrusion detection surveillance technology and personnel. Lighting also provides a deterrent to intruders by shedding light on suspicious activity, and helps to prevent covert access to restricted and protected areas.

### Maritime Assets

Preventing potential intruders from infiltrating the perimeter and boarding the platform of an offshore installation is the primary objective of securing offshore energy assets. Detecting approaching threats and crafts can be accomplished by use of short-range radar video surveillance, while night-vision and infrared (IR) cameras identify and pinpoint physical incursions and thermal anomalies. Underwater, divers and submerged submarines are detected and tracked by multibeam active sonars and sonobuoys. Employing hardening tactics such as underwater fences can deter hostile crafts from penetrating the marine security zone. Access control systems with ‘man traps’ can prevent intruders from gaining unauthorised platform access, while vectored pan-tilt-zoom video cameras provide situational awareness. An integrated surveillance intelligence system (ISIS) can provide correlated sensor communication, mitigating risk and producing faster intrusion detection and incident response reaction times.

### Pipeline Assets

Typically buried several feet underground, pipelines are less susceptible to attack than other energy assets. They run for long distances through geographically challenging terrain such as mountains, deserts, underwater and jungles, making continuous protection financially prohibitive. Detection is the primary preventative security measure that can be taken. Operators emphasise security in particularly vulnerable areas such as river crossings, control centres, junctions, manifolds and storage tanks, utilising surveillance systems based on seismic and acoustic sensors and long-range motion detection cameras. These devices detect leakage and ‘approach to line’ and are typically placed at pumping, compression and valve stations. Fibre optic networks transverse pipelines; using sensors, these networks can be tapped into to obtain operating status data. In addition, supervisory control and data acquisition (SCADA) systems used to detect

Figure 1: Physical Security Solutions in Refineries



abnormal operating conditions, such as an unexpected change in pipeline flow rate or pressure, are another key aspect of safe pipeline operation.

### Refineries

Physical security solutions in refineries are implemented to ensure the safety of personnel and assets. These solutions range from perimeter intrusion detection systems (PIDS) to access control and video surveillance monitoring. The systems collectively monitor and manage people and facilities by authenticating and authorising the access of individuals, looking for anomalies and deterring possible malicious attacks or security breaches. Access control systems, which include door controllers, egress motion detectors, keypads, readers, badges, biometric readers and time and attendance systems, form the barrier defence systems that pre-determine when and where an individual can routinely go or not go within the refinery campus. Another technology gradually being introduced into refinery security is a combination of radiofrequency identification (RFID) and global positioning system (GPS) sensor technology; this helps to track people and ensure they can be rapidly located in case of a disaster, and also ensures that they are at their assigned posts based on health, safety and environment (HSE) rules and mandates.

### An Integrated Approach

Historically, physical security solutions have taken a point-solution approach, where numerous closed-circuit television (CCTV) vendors, intrusion detection providers and access control manufacturers provide one-off or stand-alone solutions. While seemingly effective, these solutions have failed to provide a comprehensive analysis of physical security.

Based on a network-centric architecture, a C2 centre collects intelligence and information from various sensors – such as CCTV, radar surveillance, intrusion detection and access control – and other relevant sources, then processes and analyses the information to provide increased situational awareness, allowing the appropriate action to be taken. C2 systems are based on physical interfaces that use data collected from various sources. With this type of architecture, logical and physical system logs can be aggregated, analysed and correlated, allowing further investigation of unusual occurrences. Once an incident has been detected, the built-in workflow engine initiates a pre-defined response plan that drives the entire situation management process and automatically notifies response organisations (police, fire, health) and personnel. The automated nature of the system allows for tasks, notifications and incidents that are not handled within pre-defined time thresholds to be escalated for an alternative course of action. Finally, data from all of the sensors, videos

and security devices are stored in a central database to allow for forensics analysis and incident response review.

The end result is a system that provides automated planned responses to critical questions:

- What is the incident?
- How do we respond to it?
- How do we resolve it? and
- How do we prevent it from happening again?

These comprehensive data provide asset managers and platform operators with crucial information, ensuring an appropriate incident response that provides safety and security to personnel, the platform and its assets.

### Case Study

An international oil company with assets in various parts of the world began facing significant security challenges. Due to various geopolitical scenarios, its assets were repeatedly targeted for malicious attacks and abuse. The company's Chief Security Officer had a complex challenge in front of him. He had to anticipate the nature of an attack and when and where it would happen, and provide a timely and appropriate incident response that would mitigate and contain the incident on a global scale.

The company's first step towards achieving this was the deployment of an appropriately scaled infrastructure of sensors that monitored the assets based on criticality, threat, vulnerability and other risks associated with each. First, it deployed high-resolution CCTV cameras throughout its oil-producing assets, which included offshore, land-based rigs and production facilities. The CCTVs that had the ability to link thermal and visual images were also rich in features such as electronic image stabilisation, 60Hz frame rate, high-resolution pan-tilt, 30x optical zoom with auto-focus and wide area network accessibility; used lasers that provided long distance high-resolution surveillance (day or night, rain or shine); and could record in either H.264 or MPEG-4 format, which saved bandwidth and storage space. They then tied the CCTVs to an intelligent video motion detection system that had advanced video content analysis and could detect movements of objects within a specified zone, generating appropriate alarms and actions by the CCTV system.

Throughout each of the company's facilities, surveillance radar sensors were deployed as part of its PIDS. The sensors were installed mainly on fences, access gates and natural environmental barriers, and were based on spread-spectrum technology, which provided increased accuracy and consistent determination of the range of detected targets within the search beam. This technology was selected due to its immunity to interference, jamming and emissions from other radar units, and because it is virtually undetectable by conventional radar detectors or scanners. For the company, another important deciding factor in selecting these sensors was that the units produced low emissions; making them exempt from frequency licensing requirements.

In addition to sensors, the company installed fixed passive bollards and barriers in its land rig facilities where no vehicle access was needed. These bollards were certified to stop a truck weighing up to 65,000lb and travelling at 50mph. For its main entrances, where frac and wireline trucks needed access, (automated) active barriers were

selected. The company created curves and zigzag paths on main access roads as a natural impediment to slow down speeding cars and trucks. To protect its maritime deepwater drilling assets, radar surveillance systems were deployed, offering a 360° view of the facility that tracked vessel movements in numerous directions up to 5km. The company also installed pan-tilt-zoom forward-looking IR (FLIR) cameras. Based on thermal imagery, these cameras used digital image processing that provided detectability of objects radiating heat in cold environments when visibility was almost obsolete.

Finally, the company installed GPS and asset tracking technologies in remote danger zones to ensure the safety of their personnel and drilling tools with nuclear magnetic resonance (for measuring neutron and density logs). The combination of new-generation RFID tags along with GPS provided instant global location information for any of the company's tagged assets.

To obtain a comprehensive physical security view of all of its assets, the company made a significant effort to try to integrate information from all of its sources into a single, fully functional management interface that would provide situational awareness and enhance their incident response capabilities. The company decided to use a physical security information management (PSIM) console; this turned out to be key in achieving successful integration because of its ability to receive and process information from various sources while providing C2 capabilities. The PIMS system also tied into the company's existing HSE systems, ensuring that personnel entering/exiting oilfield assets had the appropriate safety training and credentials, and that they were also following appropriate HSE operational procedures related to security and safety.

Concurrently, the company's C2 centre was receiving logical security logs from the network infrastructure and logical perimeter protection tools to help better correlate security breaches and events. SCADA information was also provided to the command consul as a means of providing realtime status of exploration and production of the assets. This was important as it influenced the sequence and criticality of decisions that needed to be made in case of a security incident during drilling and exploration. The company's end result was a system with a geographical information system (GIS) interface that provided not only a global dashboard-style physical security view of all assets, but also the ability to make better informed decisions during an incident. The initial costs of the system were high, but the company's return on investment was rapidly recognised by the savings that were achieved through deterring attacks and ensuring fluid production by reducing damage to personnel and assets in the event that a security incident occurred.

### Lessons Learned

Throughout this case study, some valuable lessons in energy asset security have been learned:

- Information technology (IT) and physical security personnel are essential to designing, deploying, managing and operating physical security systems.
- Interoperability of old and new systems is a must.
- Proprietary closed security management systems should be avoided.
- The aim should be open-source systems that comply with global standards, are easy to learn and operate and efficiently communicate/interoperate with other systems.

- As the gradual migration of old to new security systems and technologies continues, point solutions that operate in stand-alone silos should be avoided.
- The amount of data processed during an incident response should be managed; using data from all sensors can cause a data overload.
- Redundant, resilient and self-healing network and power capabilities are mandated for the deployment of physical security systems.
- Forensics data should be documented and reviewed to constantly improve response and risk mitigation.
- When sending state-of-the-art physical security technology overseas, compliance with international export rules and regulations must be ensured.
- The impact if the technology were to fall into hostile hands must be considered.
- Deployment of high-end security devices must be supported and maintained in remote geographical locations, with planning for minimal on-site support and replacement training for local staff.
- Technology alone cannot be relied on. Proper personnel training, security operational procedures and documented/automated incident response plans will always prevail.
- Quarterly emergency security drills are necessary to ensure that personnel practise operational procedures in case of an incident/emergency.
- Personnel should be audited regularly to ensure appropriate security training is being undertaken and practised.
- When deploying security technology, it is important not to lose focus on business objectives.

### Relevant Additional Information

#### **Intrinsically Safe Technology**

Another important consideration for security infrastructure within energy producing assets is that they must be designed for harsh climates and poor lighting and need to be intrinsically safe (class 1, division 1 and 2 rating). Intrinsically safe equipment is defined as "equipment and wiring which is incapable of releasing sufficient electrical or thermal energy under normal or abnormal conditions to cause ignition of a specific hazardous atmospheric mixture in its most easily ignited concentration" (ISA-RP12.6). Class 1 includes flammable gases; division 1 includes environments where explosive material is present in the air at all times; and division 2 includes environments where explosive material is stored in sealed containers and explosive material is only present for short time intervals.

#### **Government Mandates**

Government mandates are also driving the need for increased physical security for energy assets. For example, the Maritime Transportation Security Act (MTSA) of 2002 is intended to protect US ports and waterways from terrorist attacks. It mandates that certain foreign-flagged vessels, such as LNG and oil tankers, entering US waterways meet specific security requirements and comply with the International Ship and Port Security Code. In addition, tankers and other high-risk vessels must be

equipped with automatic identification systems that will allow vessel tracking and monitoring while travelling on US navigable waters.

The MTSA also specifies that all US port facilities deemed at risk of a 'transportation security incident' (TSI), such as LNG marine terminals and fossil fuel processing and storage facilities, must prepare and implement security plans for deterring such incidents to the "maximum extent practicable".

Federal regulations have also been extended to ensure pipeline security. Sections 1,557 and 1,558 of the 9/11 Commission Act of 2004 relate to pipeline security and state that pipeline operators should:

- establish a programme for reviewing pipeline security information circular recommendations;
- develop and implement a plan for reviewing the pipeline security plans and inspecting the critical facilities of the 100 most critical pipeline operators;
- develop and transmit pipeline security recommendations for natural gas and hazardous liquid pipelines and facilities;
- if appropriate, promulgate regulations and carry out necessary inspection and enforcement actions; and
- develop a pipeline security and incident recovery plan.

To help ensure effective security at high-risk chemical facilities, the Department of Homeland Security issued the Chemical Facility Anti-Terrorism Standards (CFATS). Facilities are required to conduct security vulnerability assessments and then develop and implement site security plans with appropriate security measures.

Beyond the borders of the US, the US Trade and Development Agency (USTDA) has been allocating funds for port security projects around the world, aiding in the economic development of US commercial interests in developing and middle-income countries.

### Conclusion

Energy security continues to be an important topic for national and international oil companies as they continue to assess and mitigate the various vulnerabilities they are faced with in their up- and down-stream environments. To manage energy security, total situational awareness is necessary because it promptly detects potential incidents and deters and defuses them with minimal impact to assets and people. Moving forward, it is essential to employ a fully integrated network-centric C2 centre to aggregate information from various sensors that can analyse and correlate the data. When deploying such solutions, many factors need to be considered: everything from the convergence of logical and physical security to international issues dealing with export, support and maintenance. In closing, a key consideration is that technology should never be substituted for proper personnel training, security operational procedures and documented/automated incident response plans. ■

#### Bibliography

- US Department of Homeland Security, *Inspections and Surveillance Technologies*. Available at: [www.cbpc.gov/xpl/cgov/newsroom/fact\\_sheets/port\\_security/fact\\_sheet\\_cbpc\\_securing.xml](http://www.cbpc.gov/xpl/cgov/newsroom/fact_sheets/port_security/fact_sheet_cbpc_securing.xml) (accessed July 2008).
- Steinhausler F, Furthner P, Heidegger W, et al., Security Risks to the Oil and Gas Industry: Terrorist Capabilities. Available at: [www.ccc.nps.navy.mil/si/2008/Feb/furtherFeb08.asp](http://www.ccc.nps.navy.mil/si/2008/Feb/furtherFeb08.asp) (accessed February 2008).
- Bajpai S, Gupta JP, Securing oil and gas infrastructure. Available at: [www.sciencedirect.com](http://www.sciencedirect.com) (accessed August 2006).
- Command and control: [en.wikipedia.org/wiki/Command\\_and\\_control\\_\(military\)](http://en.wikipedia.org/wiki/Command_and_control_(military)) (accessed July 2008).
- Pipeline Security Regulations: [fas.org/sgp/crs/RL31990.pdf](http://fas.org/sgp/crs/RL31990.pdf) (accessed July 2008).
- Maritime Security Regulations: [www.ferc.gov/industries/lng/safety/marit-securregs](http://www.ferc.gov/industries/lng/safety/marit-securregs) (accessed June 2008).
- CFATS: [www.dhs.gov/xprevprot/programs/gc\\_1177001576714.shtm](http://www.dhs.gov/xprevprot/programs/gc_1177001576714.shtm) (accessed July 2008).