SECURING OIL'S FUTURE

New layered security strategies deter threats at LNG plants.
Report by BRUCE WADDELL

A wide range of economic factors has contributed to a boom in production of liquified natural gas (LNG) on the US Gulf Coast and West Africa. The growth in plant construction, combined with rising global political volatility, has increased the demand for more complex plant security solutions. Plant managers are also actively seeking solutions integrating both plant security and telecommunications systems to ensure optimal performance.

When you consider the common characteristics of LNG origination and production plants, it is easy to understand why they have become prime targets for crime, terrorist attack and other forces of political instability. These plants are typically located in remote areas that are easy to approach without being observed. The plants also tend to require large structures, with active components dispersed over a large area.

Advances in automation enable today's plants to be operated with minimal staffing. While minimal staffing helps reduce costs and exposes fewer employees to potential harm, it also reduces the ability to conduct visual surveillance.

National security agencies fully understand these critical security conditions, which is why they have imposed strict new security requirements on plant operators. These agencies are fully aware of how disruption of even a single LNG facility can severely impact public safety, energy supply and corporate revenue.

In this tense environment, plant managers are eager to learn how new security solutions can protect their facilities and their workers, and reduce the risk for production disruption. Let's examine the most common security concerns and the latest threat detection and threat minimisation strategies.

Understanding security threats

Threats to LNG facilities come from a variety of sources and the reasons behind them are never simple. Vehicles pass in and around these plants around the clock. These vehicles can cause unintentional damage with a simple accident, if there is a collision with piping or equipment. They can also be used to deliver intentional damage by themselves, or by carrying additional explosive materials.

Unauthorised personnel at plant sites can also cause extensive damages. These can include: vandals who are intent on tagging LNG tanks with graffiti; disgruntled workers or protesters intent on disrupting production; thieves planning to steal expensive equipment; or terrorists plotting to cause large-scale destruction and collateral damage.

In some of the LNG-producing countries, the plants are viewed as targets by groups of local citizens protesting social or political conditions.

What's more, most plants are located on waterways to accommodate tankers. These waterfronts can facilitate attacks by small boats, canoes, rafts, or even swimmers.

New strategies

Security strategies required for LNG plants are very similar to those required for high-profile office towers, sports arenas and sensitive military installations. There is no single method or technology that can completely prevent or detect every possible threat. Instead, a layered approach must be deployed to ensure adequate protection.

The first layer of security is inherent in the facility's engineering For LNG plants, the goal of effective engineering is to protect the facility from external access, using fences, berms, moats and lighting systems as perimeters.

Perimeter monitoring is commonly considered to be the second layer of security, where security officers and video-surveillance systems are deployed to prevent access by unauthorised pedestrians and vehicles. Today's video cameras are highly sensitive and can provide usable images in total darkness.

The third and fourth layers of protection – external and perimeter sensors – have become even more critical in today's tense environment. External sensors, positioned outside the perimeter fence, can detect an approaching threat before it reaches the physical perimeter.

One of the newest varieties of external sensors involves the installation of sensitive underground devices or cable outside the perimeter fence. These sensors detect vibrations caused by a person or vehicle passing over them. The most advanced cable sensor systems are difficult to detect

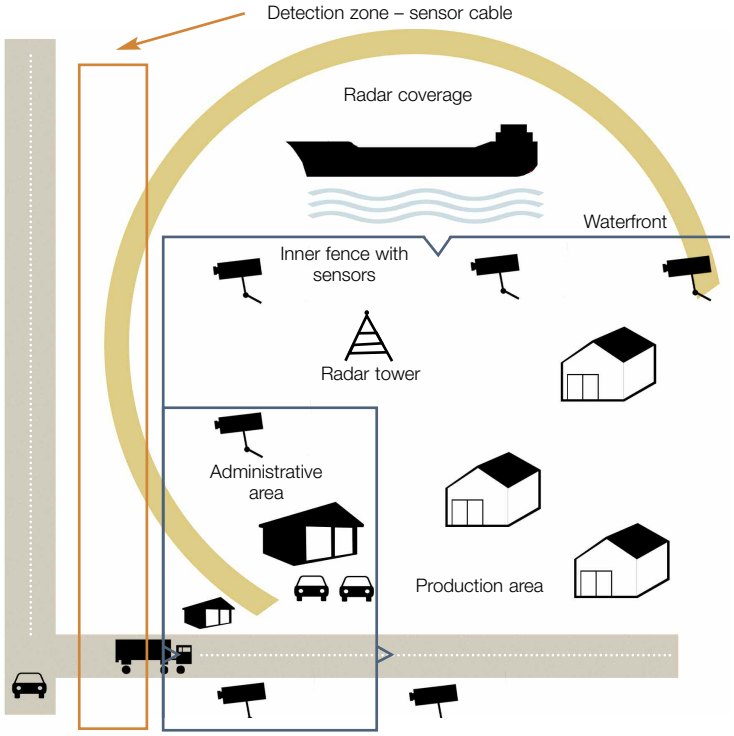
and nearly impossible to disable. Any attempt to expose them will trigger an alarm.

Other effective external sensor systems are based on microwave and radar signals. When an object passes between the microwave transmitter and receiver, the signal is disrupted – triggering an alarm. Laser systems operate in a similar fashion to microwave and radar systems, using light instead of radio signals.

On the perimeter fence, plant managers can also install sensors to detect intruder proximity, as well as the cutting, climbing or bending of the fence. These fence-based sensor systems include vibration sensors, electromagnetic sensors and taut-wire sensors. Attempts to disturb the fence will trigger an alarm. Some facilities deter intrusion by applying an electrical charge to the fence.

It's also interesting to note that video analytics can allow today's sensitive video cameras to be uses as sensors. The video images can then swiftly be processed and analysed to detect specific movements, behaviours, objects or attitudes.

In the water, active and passive sonar devices can be used to detect boats and swimmers as they approach the protected area. In extreme conditions, nets can be installed to physically block and detect underwater intrusion.



"ON THE PERIMETER FENCE, PLANT MANAGERS CAN ALSO INSTALL SENSORS TO DETECT INTRUDER PROXIMITY"

ILLUSTRATION Diagram of LNG plant security infrastructure Stratos

The challenge of integration

With the availability of so many new technologies, the challenge to develop the right solution to meet an LNG plant's security requirements can be quite daunting. That's why it is important to first perform a risk-assessment analysis. This analysis helps the plant manager identify security risks and establish the value of a security breach.

The risk assessment typically includes a site visit to analyse the facility. The analyst will examine the site for potential avenues to approach that should be monitored. The perimeter is examined to identify gaps in physical security that could allow an intruder undetected ingress. Inside the plant, high-value targets are identified for further protection. Once the review is completed, a site security report is prepared. This report identifies the vulnerabilities and flaws in the existing security infrastructure. It also makes recommendations for remediation and requirements for securing the facility.

With the findings of the risk assessment in hand, the plant manager can then engage the security systems integrator to develop the intrusion detection portion of the overall security strategy.

The integrator can also work with plant operations and security officers to bring otherwise independent systems into a coordinated system.

The most common problem with intrusion detection systems is false alarming. An excessive number of false alarms can eventually render the security system useless, as there are too many threat events to identify and evaluate. Security operators will eventually disable

sensors to ignore them, assuming another false alarm. It's also important to note that most off-the-shelf detection hardware available today is designed to operate as a stand-alone system.

This is where the systems integrator's expertise becomes most valuable. By using advanced software and alarm detection algorithms, the inputs from the various systems can be analysed – presenting to the operator only those inputs that meet pre-established criteria. For example, video cameras can be automatically positioned to provide the operator quick visual confirmation of the potential intrusion, so that appropriate action can be taken.

Leading systems integrators can also recommend solutions that integrate both security and telecommunications infrastructures. These solutions integrate perimeter security with other components such as access control, video surveillance, paging, general alarm, radio systems, computer networks and cellular services.

Telecommunications infrastructure provides the backbone on which all of these technologies can interoperate. Integration with telecommunications systems facilitates distribution of information to officials rapidly, allowing them to take quick appropriate action. Security monitoring can be centralised, utilising microwave, satellite and terrestrial media to connect the remote sites to the monitoring station. This allows the plant owner to have specially trained personnel monitoring multiple facilities, thus keeping operations personnel focused on operations.

Like an illness, intrusion is best dealt with if it is detected early. To take effective action, plant security personnel needs time to mobilise. By incorporating several layers of threat detection, the plant manager can ensure both early detection and depth of protection – making it much more difficult for an intruder to breach the protected facility.

Stratos meets communications security needs of energy industry

As the world's demand for energy increases, so does the oil and gas industry's demand for vital communications systems. These systems – which include VSAT, mobile satellite, and microwave – provide offshore vessels with reliable, high-speed data for file transfers, video conferencing, email and web access. Combined, these applications help make the network an extension of the corporate office.

With more than 700 professionals in 20 countries, Stratos Global Corp. is one of the largest suppliers of vital communications systems to the energy industry in the Gulf of Mexico, West Africa, the Middle East and Latin America.

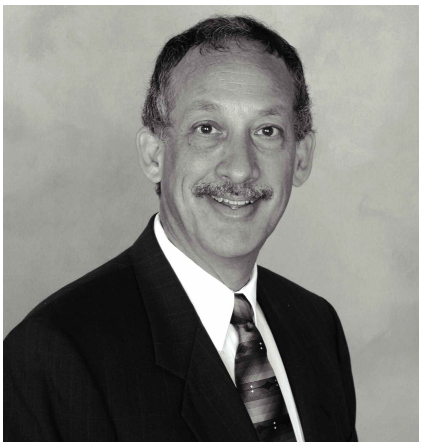
From its US offices in Houston and Lafayette, La., the Stratos Broadband Services Group operates the largest and only comprehensive microwave network in the Gulf of Mexico. The Group also has offices in Scotland, Germany and Russia.

At high-value onshore well sites, engineers depend upon Stratos VSAT networks for real-time, well-pressure monitoring. Stratos VSAT networks are also used for video surveillance applications at remote production sites.

In addition to Stratos' core communications services, the Stratos Engineering & Integration Services (EIS) team meets the total communications and security requirements of the energy, heavy construction and construction-engineering industries, including some of the world's largest LNG plants. The Stratos EIS team provides system design, installation and integration, project planning, execution and management, along with the latest satellite and microwave communications technologies.

To demonstrate its responsiveness to the energy industry, Stratos recently introduced StratosConsole, a web-based monitoring and reporting system ideally suited for energy companies using Stratos microwave and broadband VSAT networks. StratosConsole enables operators to view online the statistics and availability of network nodes and interfaces 24/7 from any location, via any Internet browser. energyfocus

INTEGRATED APPROACH The recently completed Equatorial New Guinea LNG plant, shown here under construction in 2005, utilises a unified infrastructure to support telecommunications, business networking, control systems networking, access control and surveillance Stratos



About the author: Bruce Waddell is business development manager for Stratos Global Corporation's Engineering and Integration Services team. For the past 20 years he has deployed security and telecomms solutions for both land-based and offshore energy facilities. He earned degrees in computer science and business administration from Thiel College in Greenville, Pennsylvania. He can be reached at +1 832 463 2135 or bruce.waddell@stratosglobal.com

CONTACT DETAILS Stratos Global Corporation, 1201 Louisiana Street, Suite 520, Houston, TX 77002
+1 832 463 2100 bruce.waddell@stratosglobal.com www.stratosglobal.com