

Honeywell Process Solutions



Maritime Security: Meeting Threats to the Offshore Oil and Gas Industry

Table of Contents

Introduction	3
Background	3
Security Challenges	4
Current Technology	6
Integrated Solution	7
Radar Video Surveillance (RVS) for wide area surveillance	8
Radar security cameras for threat zone assessment.....	8
Dual RVS cameras for enhanced video performance.....	9
Digital Video Manager (DVM) for alarm recording & storage.....	9
Security CCTV cameras for live facility monitoring	10
Security lighting for deterring covert actions	10
Access control for protecting restricted areas.....	10
Benefits	11
Conclusion	11
References	12

Introduction

Despite the heightened concern for energy infrastructure security—influenced in part by growing threats from international terrorism and piracy—mitigating physical security risks in the world's energy producing regions is a challenge that governments and companies have grappled with for decades.

Ensuring the safety of energy infrastructures is no easy task, whether it is in lower risk countries in Europe or North America, or in high-risk operating environments, such as those in Latin America or Southeast Asia.

One major issue for worldwide energy companies is securing manned and unmanned offshore oil and gas platforms. These critical facilities, which are intrinsically vulnerable to terrorist attack, comprise hundreds of one-off design elements, the loss of any one of which could bring operations to a sudden and costly halt.

The following paper concerns the challenges faced by the oil & gas industry in securing its vital offshore production assets. The paper discusses key requirements for an effective platform security strategy, and describes the latest technology enabling an integrated security management system.



Fig. 1. In view of rising piracy and terrorism threats, worldwide energy companies are faced with securing their offshore oil & gas infrastructure.

Background

Today, when the topic of piracy is mentioned, most people conjure up images from films such as “Pirates of the Caribbean.” These characterizations, reflecting back to the 18th century, are vastly different than the reality of modern-day piracy, which is nothing more than another expression of terrorism.

While maritime piracy most often involves the boarding of vessels on the open seas, it raises a serious concern for owners/operators of offshore oil & gas platforms. If a small group of men in a fast speedboat, with small arms and knives, can commandeer a ship with ease, what could a well-trained and determined terrorist cell with sophisticated weapons and knowledge accomplish against a highly-valued asset like an offshore rig?

Offshore installations are, in essence, hybrids of vessels and shore facilities. Though stationary, they are emplaced miles at sea away from shore-based support. Some are attached permanently to the ocean bottom and some are not. The capital investment for each installation can be enormous. The net revenues these facilities produce are equally impressive. Furthermore, one installation can handle production from as many as 24 subsea wells, which means vast quantities of crude oil are moved and controlled by a single facility.

Although the motivation for attacks against energy production operations varies—it may be to make a political statement, to gain publicity, or simply destruction for its own sake—there is strong evidence that offshore platforms will eventually become a key target for international terrorist organizations.

In April 2004, for example, three U.S. service members were killed during a maritime interdiction operation that prevented devastating strikes against two major offshore Iraqi oil terminals in the Persian Gulf. Both terminals were temporarily shut down for a 24-hour period due to heightened security concerns at a cost of \$28 million in lost oil revenue.

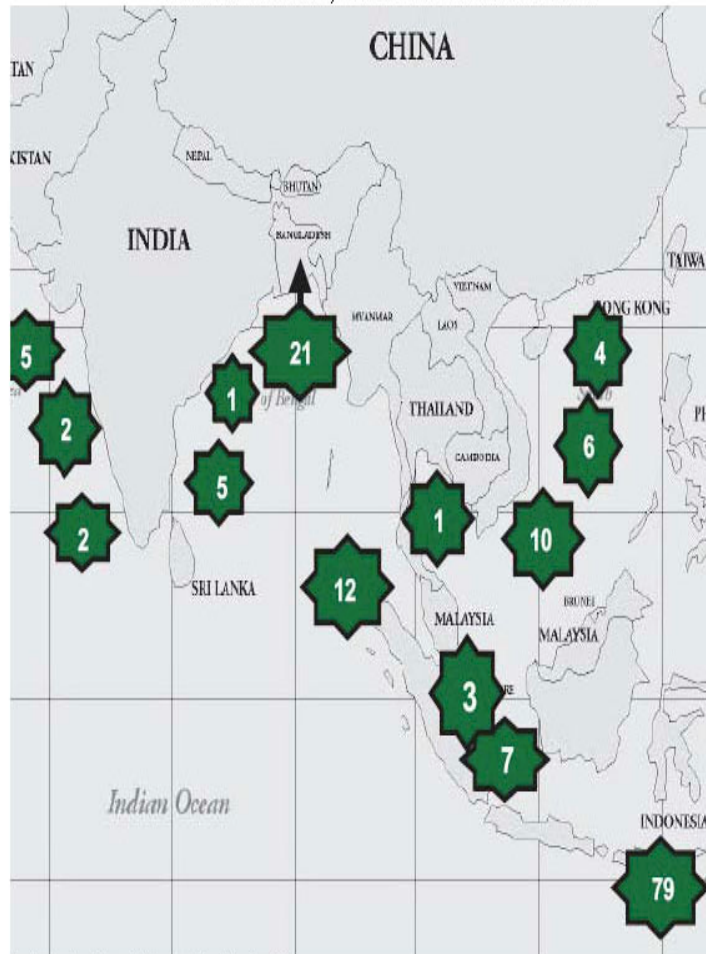
In January 2006, gunmen using speedboats invaded the Benisede oil platform operated by Shell in the Niger Delta. Several soldiers guarding the flow station were killed in the attack; five workers were injured. In addition, two staff accommodation blocks were destroyed and processing facilities damaged during the attack.

Experts in the intelligence community have repeatedly suggested that al-Qaeda and their associates could be planning a “maritime spectacular” involving the assault of a platform in the open sea. Also, there is no question international terrorist groups are fully aware the destruction of an offshore rig would create dire consequences for its owner/operator, as well as a direct and indirect financial impact in the billions of dollars on the global and regional economy.

Security Challenges

Over the next 25 years, oil and natural gas will meet approximately 60 percent of the world's energy demand, and therefore, remain the prime source of energy for industrialized and developing countries alike. Since the oil & gas industry is a major component of every national critical infrastructure, the probability for an increased number of terror attacks on energy facilities, and a higher level of their sophistication, will undoubtedly increase.

ICC International Maritime Bureau (IMB)
Piracy and Armed Robbery - 1 Jan to 31 December 2005
Attacks in S E Asia, Indian Sub Cont and Far East



Produced by the Cartographic Research Lab, University of Alabama

Fig. 2. Ensuring the safety of energy infrastructure is no easy task, whether it is in lower risk countries or in high-risk operating environments.

By their very nature, offshore installations provide inviting targets for piracy and terrorism. An offshore platform is the only type of energy-related facility that can be attacked from the surface, underwater, or from the air.

Energy companies must also be concerned with protecting facilities servicing offshore rigs, including landside and platform heliports, as well as securing support, preservation, and maintenance facilities; platform training facilities; and platform operations centers.

Typical threats to offshore operations involve hostile intruders using surface craft, diving gear or small submarines. Uninvited guests (such as fishermen), internal theft, and sabotage from contractors and employees pose additional security risks. These threats are amplified following storm evacuation until the platform is repaired and reoccupied. Petroleum development and exploration sites are frequently located in remote areas, characterized by poor transport connections and communication to the authorities and the associated security infrastructure. If national security forces are supplied to guard the site, attackers who originate from the surrounding communities usually outnumber them.

Terrorists are extremely patient and utilize their covert skills to identify gaps within offshore platform protection and strategize to exploit security weaknesses to the fullest. Historically, most attacks on the open sea occur during the late evening and early morning hours, during which time personnel vigilance is at its lowest and visibility from the platform of an approaching vessel is absolutely zero under certain environmental conditions. This plays to the strength and the most effective element of the terrorist strategy— the factor of surprise.

Due to rising security threats, offshore platforms are subject to increased physical protection as part of the framework of critical infrastructure in the United States and other countries (i.e., the airspace and approach by sea are subject to continuous surveillance and optional military intervention). However, as the terrorist attack on the USS Cole in Yemen in 2000 demonstrated, even a battle ship with its enhanced technical and operational capabilities to ward off an enemy assault has proven vulnerable to a suicide boat attack.

Large offshore facilities operating on the Outer Continental Shelf (OCS) of the United States must meet strict security regulations established by the U.S. Coast Guard and Department of Homeland Security. The 33 CFR 106.105 requirements were developed under the authority of the Maritime Transportation Security Act (MTSA), which among other things, requires the development of security plans designed to deter, to the maximum extent practicable, Transportation Security Incidents (TSIs) resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

According to the government regulations, an OCS facility owner and/or operator subject to the MTSA regulations of 33 CFR Part 106 is required to have a U.S. Coast Guard approved Facility Security Plan (FSP) in compliance with 33 CFR 106 subpart D in order to conduct MTSA applicable operations. The FSP is valid for five years from the date of its approval. Failure to have fully implemented the approved FSP is a violation of the MTSA regulations and can result in a civil penalty against the owner/operator of the OCS facility. Non-compliant operators are also subject to having their operation shut down until an approved FSP is in place.

Current Technology

In developing an effective facility security plan for offshore rigs, platform operators must achieve early detection of potential attacks as the first line of defense. This is the critical step in putting together the most cost-effective countermeasure to avoid attacks or prevent intruders from actually boarding the platform.

Offshore platforms currently utilize a number of deterrent techniques when operating in high-risks environments. These include nighttime deck patrols, spotlights to watch areas close to the rig, electrified fences, and coordination between tow vessels and the rig to share information on possible approaches.

Increasingly, electronic security components play a valuable part in securing larger manned platforms. System elements can include: Short range radar to identify vessels approaching the platform; vectored pan-tilt-zoom (PTZ) video cameras; situational awareness software (SAS) to provide a picture of where vessels are vis-a-vis the platform and other vessels, remote annunciation methods, including two-way marine radios and hailing systems, stand-off access-denial systems, including water monitors and long-range acoustic devices; close-in access-denial systems, including hardened-landing-dock gates; and weapons (in waters where lethal options are warranted).

Short-range radar serves as an effective early warning asset. It can provide warning for vessels approaching from as far as 20 miles away. These systems can be programmed and interfaced with SAS such that any vessel vectoring towards the platform will cause an audible alert. That, coupled with strategically located weather-resistant, high-resolution PTZ cameras, will ensure security gets a useful view of any approaching craft. The vessel can then be hailed by marine radio from the platform. If the vessel does not respond, the crew will ready defensive measures.

Integrated Solution

The concept of maritime security is comprehensive and covers all threats to the safety and security of offshore platforms. Therefore, it is imperative that platform owners/operators implement a comprehensive security management system to enhance security planning, implementation and operations at sea-based facilities, and to reduce the load on security personnel by rapidly processing alarm information and presenting it to the operator in a concise manner.

Effective maritime security systems integrate various subsystems (i.e., radar video surveillance, closed-circuit television, access control and intrusion detection) to provide a seamless operation. This approach is intended to provide full situational awareness at the fingertips of the platform security operator.

Major automation suppliers serving the oil & gas industry, including Honeywell Process Solutions, have developed security management solutions integrating access control, perimeter protection, video surveillance, and intrusion detection, as well as network protection and process control systems. As a result, security breaches or safety incidents are reported simultaneously to platform operators, security personnel and onshore security offices.

With alarm information presented quickly and clearly, platform personnel are positioned to evaluate potential threats and initiate the appropriate response. The speed with which workers respond to an alarm is a measurement of its effectiveness and an asset to the security of the platform; “advance awareness” of potential attacks is a deterrent to would-be terrorists in achieving their goals.

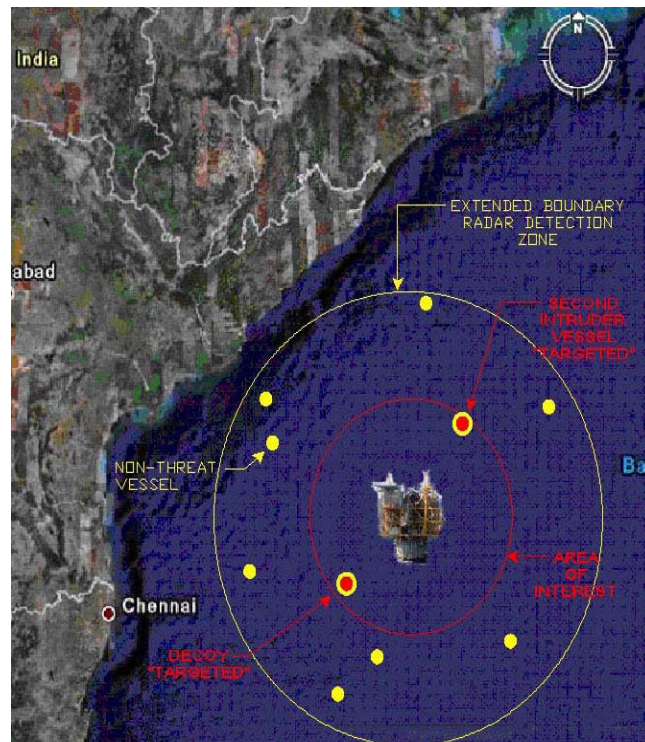


Fig. 3. The latest advancements in radar video surveillance (RVS) offer offshore facilities a larger footprint for intrusion detection.

Ultimately, integrated security management solutions enable offshore operations to implement a layered security strategy connecting process control with physical security at the facility, creating visibility at the enterprise level, and elevating the line of sight necessary to meet new threat prevention and response requirements.

The components of an integrated security management system can include:

Radar Video Surveillance (RVS) for wide area surveillance

If we look at one of the primary strategies of terrorists—to stage their attacks under the cover of darkness when security vigilance is at its lowest point—it highlights a major weakness in the protection of offshore platforms.

Humans as a rule of thumb are very poor detectors as they are prone to distractions and loss of focused attention for any period of time. With the added dimension of low or no visible light, the first indication of hostile intruders may be when they are actually on the structure. This eliminates every opportunity to deter or mitigate the boarding of the platform.

In a typical offshore environment, Radar Video Surveillance (RVS) is a key element in guarding against potential attacks. RVS provides 24/7 vigilance that is not dependent on humans, while enabling early detection and advance warning of approaching vessels within the Area Of Interest (AOI). This allows personnel to implement countermeasures such as:

- Sound alarms on the platform
- Alert the company and other counter-threat support (on-shore, Coast Guard, etc.)
- Illuminate the platform and the suspected craft
- Initiate other response procedures

The response action taken by platform personnel will clearly communicate to the approaching vessel it has been detected, thus taking away the element of surprise. In many cases, detection will serve to deter prospective attackers before they actually reach the facility.

Radar detection offers an added dimension of mitigating “decoys” and other covert tactics utilized by intruders. In this scenario, a suspected primary craft enters the AOI in order to draw the attention of security personnel and divert their focus from a second craft approaching from the opposite side of the platform, which may provide the opportunity for intruders to board the structure unobtrusively.

The latest advancements in RVS offer offshore facilities a larger footprint for intrusion detection. Radar units mounted in explosion-proof enclosures can be mounted in hazardous locations virtually anywhere on the platform, offering a 360-degree view of the facility and surrounding detection zone. Each vessel is identified within an “Extended Boundary,” while vessels within the AOI are targeted and alarmed at the security command center. With full visibility of the area around the platform, any multiple attack approaches will be clearly displayed and alarmed—providing security operations with awareness of all potential threats against the structure.

In addition, the use of object-based models for computer programming enables the properties of radar screens to be linked directly with control capabilities. That means security personnel can now treat the radar screen as if it were another camera, with the ability scan in and out and perform other kinds of radar operations typically done on a separate operator interface.

Radar security cameras for threat zone assessment

A dual-head Closed Circuit Television (CCTV) Surveillance System can be fully integrated with RVS and the security management system for visual assessment of detected targets. The Radar CCTV Surveillance System consists of a combination laser-illuminated day/night camera and a thermal camera. The use of dual cameras optimizes visual assessment under a wide range of operating conditions.

As we identified earlier, radar sensors are deployed on offshore platforms to assess specific zones of detection. The outer Extended Boundary provides situation awareness of all surface vessels within a specific range of the offshore platform. The inner AOI establishes the threat zone so when this area is breached, RVS initiates an alarm condition to the security operator. At the same time, a live video stream of the target is displayed at the operator’s monitor for evaluation and assessment of the object. If the target is deemed “safe,” then the operator acknowledges the alarm and RVS continues to track the object. If the target is of concern, the operator starts the implementation of a pre-determined response plan.

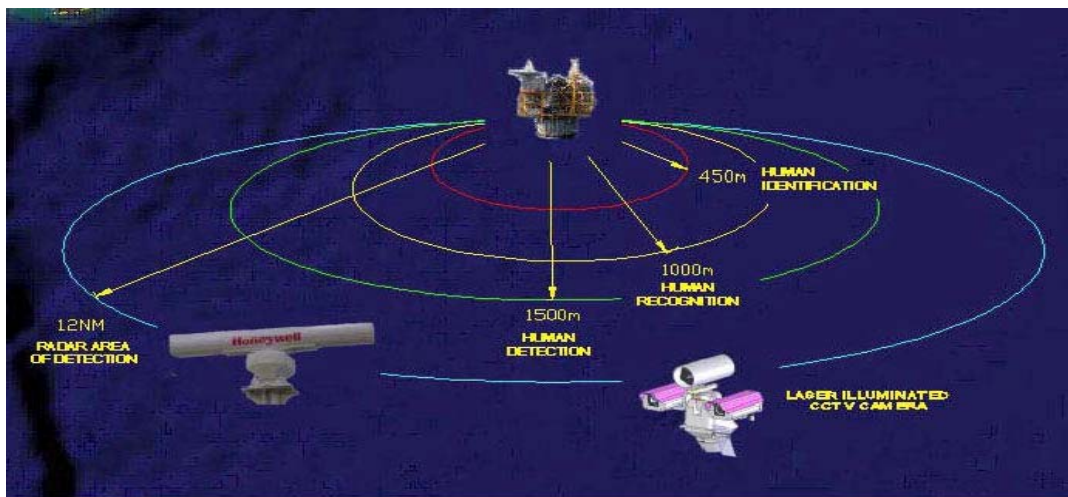


Fig. 4. Radar sensors are deployed on offshore platforms to assess specific zones of detection.

When establishing AOIs, it is important to select the appropriate security camera(s) to align the camera resolution with the assessment requirements. For example, the AOI may be established at 1500m from the platform and the selected cameras should provide detection capabilities at the same distance.

Security camera performance is based on resolution as well as the size and proximity of the object to the camera. For assessment purposes, resolution levels are defined as:

- Detection: Ability to detect the presence of the object within the AOI
- Recognition: Ability to recognize the object by its class, such as rowboat, speedboat, etc.
- Identification: Ability to identify the object as a man or women, name of the vessel, weapons that are in the field of view, etc.

Dual RVS cameras for enhanced video performance

Dual RVS cameras complement each other under adverse environmental conditions. For example, a laser-illuminated day/night camera displays objects and their features in no light conditions with natural contrasts similar to normal daylight views. The result is a day/night system with superior video quality that makes it ideal for 24-hour security threat assessment with detailed recognition. Laser-illuminated cameras can provide human detection at 1500m, human recognition at 1000m, and human identification at 450m.

A thermal camera is used to identify an object's energy in relationship to the surrounding area. In periods of heavy fog, the laser illuminator performance will deteriorate, whereas the performance of the thermal camera will excel. Thermal cameras can provide human detection at 2000m, human recognition at 900m, and human identification at 300m.

Digital Video Manager (DVM) for alarm recording & storage

A Digital Video Manager (DVM) system allows platform personnel to capture and record the cause of an alarm and perform immediate assessment. It also provides state-of-the-art video storage for fast, convenient access to important video data from any authorized workstation. Whenever possible, the video storage system should be housed in a secure environment, or at least in an unobtrusive place, so there is an increased chance of it surviving any attack on the platform. Retrieval of the video data will furnish forensic information as well as evidence in the prosecution of the perpetrators.

Video analytics is an added dimension to the security of the platform, providing a passive, covert line-of-sight for detection, surveillance and alarm assessment from a single CCTV camera. Its value is in detecting human body movements, whether they are in a stairwell case or corridor, or restricted area. Video analytics is only limited by the camera's field of view. The DVM analyzes the video stream 24/7, and upon detection, immediately notifies security for assessment—reducing response time.

The DVM's functionality, through integration, should extend to the enterprise network, allowing a single system to manage all CCTV surveillance for both security and process operations. The system provides recorded and live video to on-shore corporate facilities or emergency response teams, enabling them to analyze current events and develop appropriate response plans. During periods of heightened vigilance, security video can be a shared responsibility among various process and security operators throughout the offshore platform.

Security CCTV cameras for live facility monitoring

Security CCTV cameras have two important roles in an overall security plan for an offshore platform. The first role is assessing any detected alarm and validating the root cause of that alarm. The second role is that surveillance; the cameras utilize a live video stream to continually monitor activity approaching the platform, or an area on the platform, and to direct the response force to counteract and confront the intruder.

Platform owners/operators should consider providing CCTV camera coverage for the following areas:

- Main accesses to the platform structure
- Vulnerable and critical areas not under direct supervision
- Radio room
- IT main server room
- Main electrical room
- Access points between decks
- Other critical areas

Security lighting for deterring covert actions

Facility lighting is an essential part of an integrated physical security program. A well-lighted area is a deterrent to intrusion, reducing the advantages of covert actions and making the job of the saboteur much more difficult.

Lighting should be installed in all vulnerable areas of the platform, as well as any area subject to night infiltrations. Security personnel should carefully consider the number of lights or at the least the placement of lights around the platform, especially in areas of platform access.

Security lighting allows security and operations personnel to maintain visual observation of the platform during the hours of darkness. Lighting integrated with CCTV cameras and video analytics in the overall security posture provides enhanced security and effective coverage of the platform without the addition of personnel.

Access control for protecting restricted areas

An effective and robust access control system is a requirement on any offshore platform. Its primary purpose is to prevent subversive activity, such as sabotage and any other action adversely affecting the platform operation. Platforms should start by establishing multiple restricted areas secured and controlled at all times. All alarms—denied access, forced entry and door-held-open-too-long—should be immediately investigated. Areas requiring higher level of security should be complemented with the addition of CCTV cameras for immediate assessment.

Platform areas that should be considered for restricted access include, but are not limited to:

- Radio room
- Local equipment rooms
- Electrical rooms
- IT hubs
- MCC rooms
- UPS/battery rooms
- Instrument/DCS hubs
- Sub-level access to platform

In areas where the safety of personnel or operations and security are in conflict, safety must always take precedence. Where access control is in conflict with safety, platform owners should consider an alternative security measure implementing alarmed monitoring of an area entry combined with CCTV video imaging. This approach enables an alarm event, coupled with the location of the alarm with a live video stream, to be displayed on the security console so personnel can immediately assess the validity of the potential threat.

Benefits

Thanks to recent developments in maritime security, offshore oil & gas facilities now have the best technology possible to prevent, detect, deter and respond quickly to a wide range of security threats and breaches. Integrated security management systems detect threats and incidents earlier, so response time is improved. In addition, they merge data to create more robust knowledge that enables more efficient actions with fewer resources.

A unified operator interface makes it easier for platform personnel to evaluate potential threats and take appropriate action without having to consult displays on multiple user stations. Personnel gain confidence that functions are performed the same way at each station—with the same set of controls. Workers who have multiple roles at a facility are better able to do their jobs and deal with security situations that may arise.

Since the integrated security infrastructure has a common look and feel, engineering costs are reduced. This approach also minimizes capital expenses in terms of the number of servers, software packages and spare parts required for the system.

Finally, implementing an integrated security management solution gives platform owners/operators one supplier to work with for all system maintenance, training and support.

Conclusion

Offshore oil & gas installations may soon become the target-of-choice for international terrorism, irrespective of the political system and social-financial boundary conditions of the society under attack.

In response to the threats posed by piracy and global terrorist groups, oil & gas companies must take decisive action to ensure the safety and security of their vital offshore assets.

A comprehensive security management system, incorporating the latest automation, surveillance and alarm technologies and integrating a common user interface for security and operating personnel, offers an effective solution for the growing security challenges in today's offshore operating environment.

References

- House of Commons, Transport Committee, Piracy, Eighth Report of Session 2005–06; HC 1026, Published on 6 July 2006,
- by authority of the House of Commons, London: The Stationery Office Limited, £0.00.
- Maritime and Coastguard Agency: Marine Guidance Note 298(M).
- Thackrah, John. Dictionary of Terrorism, Routledge Publishing, 2003.
- Crocker, Michael. "Platforms, Pipelines & Pirates." Security Management 1 June 2007 <<http://goliath.ecnext.com>>.
- Steinhausler, F., Furthner, P., Heidegger, S., Rydell, S. and Zaitseva, L. "Security Risks to the Oil and Gas Industry: Terrorist Capabilities." Strategic Insights, Feb. 2008 <www.ccc.nps.navy.mil>.

For More Information

To learn more about Honeywell's security solutions, visit our website www.honeywell.com/ps or contact your Honeywell account manager.

Automation & Control Solutions

Process Solutions

Honeywell

2500 W. Union Hills Dr.

Phoenix, AZ 85027

Tel: 877.466.3993 or 602.313.6665

www.honeywell.com/ps

WP-08-14-ENG
May 2008
Printed in USA
© 2008 Honeywell International Inc.

The Honeywell logo, consisting of the word "Honeywell" in a bold, red, sans-serif font.