One of the top priorities for any manufacturing operation is safety—not only the safety of workers in the plant, but also of the people living within the surrounding community. Just as safety practices and equipment must evolve to respond to changes in working conditions and regulations, the world of industrial security is changing in response to rising global threats.

Today, companies have an urgent need for a physical security strategy that can help protect their assets from potential threats. A growing number of vulnerabilities require an integrated security system that enables faster actions with fewer resources.

Vulnerable industrial operations
Growing threats demand an integrated strategy

By Adrian H. Fielding

hpsmarketing@honeywell.com
need to make improvements to their overall security practices and systems to protect intellectual and physical assets. From the physical perspective, users require a solution that integrates multiple security technologies. This facilitates automated processes that give the ability to deter, detect, delay, deny, and defend—and thus prevent and mitigate a wide range of potential hazards.

Industrial facilities of all sizes can use the power of automation to meet current legislative requirements while enhancing safety and optimizing their long-term security model.

Background
The industrial sector faces real challenges as technology is always advancing, experienced professionals are retiring, and the business environment of the new global economy imposes ever-greater competitive demands. At the same time, moral, regulatory, and insurance requirements must be met in terms of maintaining a safe and secure workplace.

Traditionally, industrial firms have been focused on safety and productivity. However, recent threats to critical infrastructure have prompted a tightening of security measures. Reducing vulnerabilities to plant automation systems and other critical assets is necessary to help ensure the safety, reliability, integrity, and availability of these systems.

The hazards of the post-9/11 world have spurred industry and government initiatives aimed at enhancing the security of industrial facilities in ways that meet nontraditional threat scenarios. As with cybersecurity, the basic concept of physical security is to detect vulnerabilities and prevent an intrusion. Even though it is a different kind of intrusion, the consequences of failing to provide adequate protection can be disastrous.

Common industrial security risks include workplace threats, violence, theft, pilferage, counterfeiting, sabotage, terrorist attacks, trespassing, activist disruption, vandalism, and contamination. Many manufacturing facilities are fairly accessible, and employee security awareness is often lacking or weak.

Theft is a particularly important concern during new greenfield projects or plant expansions. A 2011 report by the National Insurance Crime Bureau indicated that in the U.S., $300 million to $1 billion a year is lost to the theft of construction equipment and other high-value materials.

Even the tightest plant perimeter security, while important, cannot ensure protection against a determined attack. Therefore, companies need to implement new and innovative solutions covering the entire scope of physical security requirements.

Today’s security challenges
It is no secret that many kinds of industrial facilities have been identified as potential targets for malicious attacks, including oil and gas production sites, refineries, gas distribution sites, chemical plants, pulp and paper mills, and power-generation stations. As such, there is a need for a comprehensive security strategy for these facilities and other critical infrastructure.

Government regulations such as the Chemical Facility Anti-Terrorism Standards and the Maritime Transportation Safety Act also require companies to implement effective measures to defend against industrial security threats. There may also be a further need for mandates, such as the transport worker identification credentials.

To help safeguard physical and human assets, production plants and other vulnerable operations require an integrated security system that brings together multiple security technologies. These technologies must be able to communicate in real time, merging data to create new, more robust knowledge for faster, more efficient actions with fewer resources. Physical security measures represent important considerations in an asset protection scheme that includes cybersecurity and information security. It is impossible to completely separate the different aspects of an overall plant security posture. Preventing attackers from gaining access to the site may also bar them from access to critical process control networks.

Current physical security requirements include:

- identifying and controlling individuals who enter and exit the facility
- tracking movements of building occupants and assets
- controlling access to restricted areas
- tracking and locating equipment, products, and other resources
- tracking the location of personnel on site in the event of an incident
- integrating control and security systems for greater speed and efficiency
- protecting process automation networks and systems from potential intrusion
- responding quickly to alarms and events

The U.S. Department of Justice has determined that an effective plant security system serves three vi-

Honeywell

hpsmarketing@honeywell.com
In the industrial sector, recent threats to critical infrastructure have prompted a tightening of security measures. Employing robust tools, such as video surveillance, access control, perimeter intrusion detection, and command centers, that work together for an effective method of protection for industrial facilities. Although many of the tools have been in use as stand-alone capabilities for some time, the ability to merge them in a unified system adds substantial synergies and benefits.

Having such an integrated physical security solution allows plant managers and operators to ensure their top safety priorities are met while concentrating on other components of the safe, secure operation of a facility. With this strategy, certain layers of protection can deter incidents in the first place, while others can provide detection, alerting, and associated guidance. The approach enhances important security functions, such as access control for real-time mustering during an emergency. Plants are no longer faced with checking names off a paper list, but rather use solutions like automated badge readers to confirm workers have reached safe haven.

For many industrial facilities, however, seeing the “big picture” of operations can be difficult. Multiple data sources, collaborative issues, contextual awareness, safety, and security make up a complex ecosystem that is often hard to manage. Modern “command and control” systems meet these challenges by integrating facility-wide safety and security resources and making them available via a collaborative human-machine interface (HMI). This solution reduces the disconnect between operational silos and unites them under a common goal. Users can zoom in and out of specified views to obtain detailed information. Additionally, multiple people in multiple locations can sequence the best possible response, in order of priority, to a security situation.

Advanced incident workflow tools guide plant personnel through the decision-making and response process during critical situations. By seamlessly integrating emergency operations with safety and security systems, they help reduce risk, promote continuity, and increase productivity. For instance, authorized users can perform a number of actions from a single mass notification to key people or personnel affected. This includes automated or manual control of surveillance cameras, or unlocking and locking doors or gates to allow first responders to access critical areas.

The first step in any plant-wide security initiative is a site vulnerability assessment to determine possible gaps in protection. The cornerstone of determining a facility’s needs is to understand its site. Organizations must have an acute awareness of not only the plant’s physical layout, but also of how employees act within that environment. The assessment will further examine the impact of a security breach and the effect it can have on security personnel and process operators. Lastly, a thorough understanding of the latest security technology is necessary to determine threat mitigation steps and how to fill the observed security gaps.

While mitigation steps are unique to each site, practices like integrating...
process control and security systems can strengthen the situational awareness of process and security personnel. Security personnel are made more aware of nonsecurity incidents, and process personnel are made more aware of security incidents.

**Integrated technology**
Increasingly, designers of process and building automation systems are utilizing a consistent system and application architecture. The result is a unified solution for control, safety and security, whereby video surveillance, access control, and perimeter detection are tightly integrated with alarms and events raised in process and safety systems for intelligent, coordinated responses. An HMI with a common look and feel results in better, faster decision making. Both control room consoles and security office desktops have visibility of events. This approach also minimizes complexity during all stages of system implementation, operation, and maintenance.

If there is ever an incident on site, everyone (security and process employees) knows about the incident in real time. Plant management can get the right information to the right people quickly and go into action immediately. This reduces risk and enhances not only security, but also safety.

Video surveillance via server-based digital closed-circuit television (CCTV) is a critical component of any integrated security program. It is typically used for two purposes: overall surveillance at the plant perimeter and critical interior locations, and for process monitoring, such as flare stacks or rail car unloading. CCTV systems may employ explosion-proof cameras for hazardous process environments or tamper-resistant cameras for high-traffic areas.

Intelligent video systems enable the control and security departments to use common cameras in an emergency situation. However, operators only view the images they need to see related to a security or process event. These systems also offer “picture-in-picture” capabilities for simultaneously monitoring security and production activities in different locations. In some facilities, the operations team is required to oversee security and perimeter access during overnight hours and other periods of minimal staffing.

Centralized recording, remote off-site surveillance, and video backup can enhance an intelligent video system. Personnel can specify when and what types of recordings they want captured. Recorded images can include not only the incident, but also what happened immediately before and after, providing a complete picture to enhance the investigation process and outcome.

Motion sensors, thermal video systems, and other industrial-quality sensing devices further support the CCTV solution. For example, smart digital cameras tied into the plant alarm system detect motion throughout the site—if a human intruder is detected, an alarm sounds and displays. Control room operators and security officers receive the alarm notice if the intruder is located near sensitive process plant equipment.

Experience has shown digital CCTV surveillance increases se-
curity and operational efficiencies; automated event detection improves operator responses, acting as the next generation of process sensors. With a common video solution for both security and control users, it also allows increased situational awareness and reduced system costs, complexity, and equipment.

Benefits of a holistic solution
By deploying a holistic solution to meet the needs of both security and process operations, industrial organizations can significantly reduce risk, mitigate threats, and increase their overall asset protection preparedness. Integrated systems detect incidents earlier, so abnormal situation response time is improved. By using systems with the same look and feel, engineering and training costs are also reduced.

An improved physical security posture can also help safeguard corporate image; companies manage security for fewer incidents and improved safety. Indeed, this approach is the foundation for protecting lives and assets within an industrial setting. Video surveillance triggered by events and alarms means better emergency response, improved awareness, and faster mustering. The availability of historical data from these systems showing events, alarms, and associated responses helps document proper operating procedures and demonstrate regulatory compliance.

A manufacturing plant with tighter security, which only permits access to those people with the appropriate skill level for an area, decreases liability risks. Monitoring assets continuously throughout the facility helps reduce intellectual property loss, and decreases lease and capital expenditures.

Finally, improved security is synonymous with greater productivity, because securing construction sites and lay-down areas with trip-wire video analytics reduces the risk of theft, which, in turn, helps ensure prompt startups and uninterrupted production. And integrated solutions mean lower maintenance costs, greater efficiency, and improved profitability.

Approaching physical security without a plan usually results in a disjointed effort. Many industrial operations have spent tens of thousands of dollars on fencing and barricades, while failing to recognize the need for greater collaboration amongst those parties who must recognize and respond to security threats affecting the facility’s well-being.

An integrated approach to physical security starts with conducting a valid vulnerability survey, understanding a facility’s requirements, and using the time-tested concept of deter, detect, and delay. It also relies on a layered solution that connects process control with physical security at the plant, creating visibility at the enterprise level and the line of sight necessary to meet new threat prevention and response requirements.

Today’s advanced technology can deliver a common view of vulnerabilities to process control and security personnel, and provide protection from the process control room to the plant perimeter—thus safeguarding all assets of a production operation. ■

ABOUT THE AUTHOR
Adrian H. Fielding (Adrian.Fielding@Honeywell.com) is the business leader for industrial security solutions and works in the global marketing team within Honeywell Process Solutions. Fielding has been part of the global industrial security initiative with Honeywell since 2006. He is responsible for coordinating Honeywell’s strategic partners, business development, and strategic marketing of key solutions for the protection of large and medium operations, including pipelines, refineries, power plants, chemical plants, on- and offshore facilities, and industrial ports. Before rejoining Honeywell, Fielding was the integrated systems division manager for Swiss security products manufacturer, Kaba. Fielding has a strong technical background due to his 10 years of service as an avionics engineer with the Royal Air Force.

Honeywell
hpsmarketing@honeywell.com