

Honeywell Gets Physical with Security

How much can you afford to lose?

By: [Bill Lydon](#), Contributing Editor

While there is a great deal of legitimate concern about cyber security, many industrial facilities may be at high risk due to poor physical security. In today's challenging times, many kinds of industrial facilities have been identified as potential targets, including chemical and petrochemical plants, oil refineries, liquid and natural gas distributors, pulp and paper mills, mining operations and pharmaceutical plants. There is a need for a comprehensive security strategy for these facilities and other critical infrastructure. Honeywell Process Solutions' industrial security initiatives go beyond cyber security to address physical plant security.

FBI statistics for 2006 reported property crimes accounted for an estimated \$17.6 billion dollars in losses.

Honeywell Process Solutions' initiative involves working with plants to improve physical security using new technology and sound security methods.



Honeywell has a long history in the security industry with a \$3 billion security products business. With this industrial security initiative, Honeywell is now applying their expertise to the industrial process industry.

Industrial security has always been important, but since September 11th there are additional security risk concerns from terrorists. Analysts say the demand for access controls and other electronic security systems is expected to rise by an average of 7.8 percent per year to \$15.6 billion in 2012, according to a recent report

issued by The Freedonia Group. The security of manufacturing and industrial plants (as well as food and beverage production, processing, warehouse, distribution, facilities and operations), is an issue of significant importance and much misunderstanding. Industrial and manufacturing security risks include workplace threats, violence, theft, pilferage, counterfeiting, sabotage, terrorist attack, trespassing, activist disruption, vandalism, and contamination. Many industrial facilities are fairly accessible and employee security awareness is often lacking or weak.

Honeywell's Jon Harmon, Global Director of Critical Infrastructure Protection, and Steven E. Roberts, P.A. pointed out, The Defenders Dilemma, in a presentation at the 2008 Honeywell Use Group meeting:

"The defender must defend all points; the attacker can choose the weakest point."

"The defender can defend only against known attacks; the attacker can probe for unknown vulnerabilities."

"The defender must be constantly vigilant; the attacker can strike at will."

"The defender must play by the rules; the attacker can play dirty."

Security is different than process control in that you can anticipate things we expect will happen but cannot foresee all the possibilities.

In addition to terrorist threats increased risk of loss from theft is always changing. Consider the recent dramatic price increases in commodities such as copper, making it attractive to thieves. In a recent case, 800 pounds of copper wire stolen from Duke Energy would yield \$1,000 - \$2,000 in cash at a scrap yard. Copper theft has become so big there is a WEB site showing actual videos of copper thefts: [Copper Theft Videos](#)

Critical Infrastructure Protection (CIP) Initiative

Honeywell Process has added security specialists to work with their process industry experts as a resource for customers. This is part of a broader Critical Infrastructure Protection (CIP)

initiative throughout Honeywell Automation and Control Solutions (ACS) focused on Airport, Maritime, Metro Rail, Industrial, Government, and Public Events security. This means that the groups will share resources and expertise as required.

Integrated Approach

Honeywell is taking an integrators role in many process industry security applications to insure customers gain the most value from their investment. Because of the company's unique background in process control and building automation the integration of the DCS with security is straightforward. Honeywell also provides customers after market security maintenance services to insure they continue to leverage their investment in security. Honeywell can tie in the security to the process control system to simplify operations.



In a recent conversation, Harmon commented, "it was a natural fit for us to take our security products and security solutions to the process industry." Harmon went on to describe how Honeywell takes a layered

approach to security so if a "bad guy gets through the first line of defense there are other measures." The idea is to start with perimeter protection, asset control and then security inward into the facility. Asset protection is also part of an integrated security approach using Honeywell's OneWireless system on equipment and production materials.

Products

Honeywell has a wide range of security products including the following worth noting.

Access Control

The Honeywell Temaline is an established access control system is based on able to integrate with CCTV, Fire, HVAC, Asset Management, Time and Attendance and many other functions.

Radar Video Surveillance (RVS)

The Honeywell RVS system is a Wide Area Surveillance System supported by radar and other sensors to automate detection and tracking of potential threats to your facility.

When an intruder breaks your user-defined rules, RVS generates an alarm, automatically directing a video camera to the threatened area. Video is recorded and distributed over a Local Area Network to provide a recorded history for future reference or evidentiary purposes.



Video Analytics

Video analytics is an exciting technology using software to recognize security issues by analyzing video in real-time. Honeywell is applying video analytics where software analyzes unusual patterns to initiate alarms and draw an operator's attention a monitor. This solves a major problem in video surveillance where it is difficult for an operator to accurately watch many screens at once and determine when there is a security problem. For example, video analytics applied to a camera monitoring a fence line can discern the difference between animals and humans at the fence line. If a human is detected, an alarm will alert the operator.

Honeywell Plant Security

Honeywell's approach to protecting its Specialty Materials Chemical site in Geismar, Louisiana is an example of security for a process plant. The system employs a comprehensive strategy that seamlessly integrates the physical, electronic and cyber layers of security with building automation, security and process control systems, enabling the sharing of real-time information. Integration achieves faster, better responses, including pre-emptive shutdown/safe-mode and the mustering of personnel in safe areas. The Honeywell integrated security solution at the Geismar plant supports the following capabilities:

- Monitoring and protecting the perimeter with intrusion detection and advanced sensor technology.
- Providing "beyond the perimeter" surveillance - including radar tracking of vessels.
- Identifying and controlling who enters and exits the facility.
- Preventing unauthorized access by matching visitors and contractors to federal "watch-lists."
- Tracking movements of plant occupants, and quickly locating equipment and other assets electronically.
- Controlling access to restricted areas, including enhanced control room security measures tied to Department of Homeland Security threat levels.
- Improving emergency response time through early warning systems and shared alarms.
- Preventing theft of assets and chemical sources.
- Assessing site security and design solutions that meet proposed legislation, including contingency and emergency response plans.
- **Integrating systems for greater speed and efficiency.**
- Protecting process automation networks and systems from cyber threats.
- Tracking and monitoring vehicle and hazardous materials movements and storage.
- Tracking the location of personnel and visitors on site through automated mustering.

Resources

Homeland Security

Homeland Security has information on initiatives for chemical, maritime, and transportation on their WEB site:

Chemical Facility Anti-Terrorism Standards (CFATS)

http://www.dhs.gov/xprevprot/programs/gc_1169501486179.shtm

Maritime Transportation Security Act (MTSA)

http://www.dhs.gov/xnews/releases/press_release_0282.shtm

Transportation Worker Identification Credential (TWIC)

http://www.dhs.gov/xnews/releases/press_release_0558.shtm

Honeywell

[Security Resources Brochure](#)

[Intelligent Video Analytics Demonstration Video Clips](#)

As published on Automation.com at: <http://www.automation.com/get-physical-with-security>