

# Panduit Employs Multiple Technologies to Create a Security Showcase at its New World Headquarters Facility



*Panduit uses multiple technologies to connect the many security and safety devices at its new world headquarters facility*

The new Panduit World Headquarters building demonstrates the power of integrated, IP-based physical security solutions to accelerate event detection and response, enable collaboration between a private company and public safety agencies, and increase operational efficiency. Founded in 1955, Panduit develops and provides physical infrastructure solutions that enable customers to connect, manage and automate their communications, computing, power, control and security systems. Panduit solutions apply Unified Physical Infrastructure (UPI) principles to manage the risk and complexity associated with system convergence and integration, while also reducing cost and improving sustainability. The company operates in 120 countries and

makes its headquarters in Tinley Park, Ill. Areas of focus include data centers, connected buildings and industrial automation.

#### The Challenge

When planning its new world headquarters building — completed in early spring 2010 — Panduit wanted the facility to showcase its UPI vision. The building's IP network would be the platform for physical security, collaboration and energy efficiency. "You have the opportunity to build a new headquarters building only once in a career, and we wanted the building to continue meeting our business needs for 30 years," says Darrin Norbut, senior manager for workplace resources.

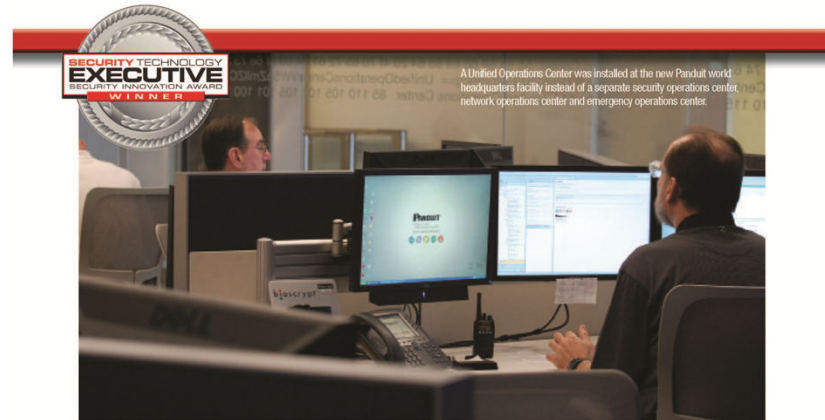
Main physical security objectives included:

- Building the foundation to centralize security operations for all 120 global offices;
- Creating a virtual fence around the 52-acre property instead of a physical fence, to automate intruder detection while lowering costs;
- Enabling collaboration with local fire and police departments;
- Increasing operational efficiency for the physical security organization by not having to maintain a separate employee database for the physical access control system;
- Maintaining physical access controls even in the event of a power outage; and
- Taking advantage of video analytics software in novel ways, such as preventing one person from "tailgating" an employee who has swiped an access card.

#### The Solution

Collaborating with N2N Secure (strategic physical security consulting), IPVision (systems integration) and Cisco, Panduit designed a state-of-the-art IP-based physical security system combining video surveillance, physical access controls and interoperable communications with employees and first responders, using any device. The IP-based system gives Panduit the flexibility to use open standards-based systems from any vendor.

The foundation of the connected building includes Panduit's own physical infrastructure solutions and Cisco wired and



wireless networks, which provide coverage throughout the entire 280,000 square-foot facility. Other solution components include Cisco Video Surveillance, Cisco Physical Access Control and the Cisco IP Interoperable and Collaboration System (IPICS). IPVision, a Cisco Premier Certified Partner, integrated these systems with each other and with Panduit's existing databases to accelerate awareness of events and automate response. N2N Secure recommended a Unified Operations Center instead of a separate security operations center, network operations center and emergency operations center (*Editor's Note: For more on Panduit's UOC, please check out the May cover story of STE, which is available in our online magazine archives — securityinwatch.com/magazine/ste/archives*). The combined workspace eliminates the cost of redundant servers and networking systems, and also enables the teams to collaborate more closely for increased operational efficiency. For example, security operations personnel can more quickly find out if an alarm from a building system resulted from a power outage, reducing time spent investigating false alarms.

#### IP-Based Video Surveillance: A Virtual Fence

At Panduit headquarters, 120 Cisco IP Video Surveillance cameras monitor the building perimeter and restricted areas within the building. Authorized personnel can monitor live and archived video

streams from any web browser on a PC or smartphone, through the supplier's Video Surveillance Manager.

Panduit used the video surveillance solution and video analytics software to create a virtual fence, saving the considerable expense of installing 4,725 feet of perimeter fence. Ordinarily, consoles in Panduit's Unified Operations Center display feeds from up to 16 cameras. If a camera detects an intruder crossing the "virtual tripwire," it signals the Video Surveillance Virtual Matrix to display the live feed from that camera in full-screen mode. A nearby Axis pan-tilt-zoom (PTZ) camera tracks the intruder, providing situational awareness so that Panduit security personnel can plan the appropriate response. At the same time, Video Surveillance Manager sends a message to the Cisco Physical Access Control system to lock exterior doors, and signals the IPICS to dial nearby security managers and play a prerecorded voice message.

Panduit also uses the video surveillance solution to identify tailgating, a traditional vulnerability of access control systems. Surveillance cameras monitor all entrances, and if the video analytics software recognizes two or more people within a certain distance of each other, the camera sends an alert to Panduit's Unified Operations Center. Security personnel can review the video from that camera with just a few clicks to determine whether to dispatch an officer to investigate.

#### IP-Based Physical Access Control: Enabler for Private-Public Partnership

The Physical Access Control system protects exterior doors, gates and restricted areas. IPVision also integrated the Cisco Physical Access Manager with Panduit's fire system so that it receives trouble, full fire and water flow alarms. When it receives a water flow alarm — unlikely to be a false alarm — Physical Access Manager signals the IPICS, which automatically establishes a virtual talk group including Panduit security personnel and local fire and police personnel. People can join the talk group using any type of radio as well as cell phones and desktop phones. The IPICS dials the phones through Panduit's Cisco Unified Communications Manager system.

Similarly, an activated fire alarm can trigger an IPICS policy to instruct the Physical Access Manager to open the gates for fire trucks. Ordinarily, firefighters must insert a key in the main gate to gain entrance. Eliminating this step enables firefighters to begin mitigating damage 30 seconds earlier. The same IPICS policy, triggered in response to the fire alarm, signals the Cisco Digital Signs solution to begin displaying evacuation instructions on Cisco LCD Professional Displays deployed throughout the building.

The IPICS enables Panduit personnel and fire, police and emergency medical services personnel to communicate directly, using any type of radio as well as a telephone, mobile phone or PC with special

# SECURITY TECHNOLOGY EXECUTIVE



*In Recognition To*

**Jeffrey Woodward**

Senior Manager  
Global EHS & Security

**PANDUIT**

*For*  
Most Innovative  
Security Project of 2010

SECURITY TECHNOLOGY  
**EXECUTIVE**



*In Recognition To*



*For*  
Most Innovative  
Security Project of 2010

SECURITY TECHNOLOGY  
**EXECUTIVE**



*In Recognition To*

**IPVISION** 

*For*  
Most Innovative  
Security Project of 2010

SECURITY TECHNOLOGY  
**EXECUTIVE**