



Advancing Airport Security

May 1, 2005

BY MICHAEL FICKES

A \$12 million initiative at San Diego International Airport aims to build wireless and fiber-optic networks that link technologies controlling access and conducting surveillance around and inside the airport.

The initiative will create a technology ring around the perimeter of the airport employing radar, thermal imaging, infrared imaging, access control systems and intelligent closed circuit television (CCTV). The technology will feed information into a security operations center that will evaluate data and dispatch people automatically through e-mail, cell phone and PDA links.

Recently introduced intelligent CCTV software called SmartCatch, supplied by **Vidient Systems Inc.**, Sunnyvale, Calif., will form a key component of the system. Currently undergoing a pilot test at the airport, SmartCatch is managing cameras at four access points leading to sterile areas of the airport.

"Right now, we are working with Vidient to build a system that will monitor behaviors related to our protocols for proper access through access controlled points," says Mark Denari, director of aviation security and public safety with the San Diego County Regional Airport Authority, the entity that owns and operates San Diego International.

For example, to boost efficiency, San Diego International policy allows airport workers to move through certain controlled doors as groups. The first person presents an ID card and opens the door. This individual monitors others on the team as they enter. Each, however, must show an access card to the reader and get a green light. The system speeds progress because it does not require the door to close between entries.

"We allow more freedom in this than some airports," Denari says. "But if someone fails to show an ID and tailgates, we want to know about it."

The access control system is not set to catch such a breach. But SmartCatch is. It can tell the difference between people and things and will note that a person has moved through the door. All along, the access control system sends data about valid card presentations to SmartCatch. If SmartCatch sees a person go through a door, but does not receive information saying that a valid card was presented, it will alarm and post video of the event on a monitor in the security center. In short, SmartCatch will alarm on breaches in the airport's door access policies. It will also catch incidents of true tailgating.

"I can't provide details, but in our pilot test, SmartCatch has detected breaches and enabled airport security to resolve the problems," Denari says.

Another SmartCatch feature will enable cameras around the airport perimeter to alarm on the presence of suspicious vehicles. One of the threats faced by airports involves large bulk explosives conveyed by truck. With SmartCatch, Denari can create virtual CCTV access points that will find large vehicles parked for a certain period of time or moving at high speeds.

"Our strengths are object tracking and object classification," says Brooks McChesney, CEO of **Vidient Systems**. "For example, it is difficult for a video system to tell if two people approach each other and cross paths or meet, turn and go in another direction. SmartCatch can tell the difference and track individuals.

"In terms of object classification, it isn't good enough to know that something is moving from here to there," he continues. "You need to distinguish between things and people. SmartCatch can tell the difference. We can also look at vehicles by size. Finally, we can integrate video with other sensing devices - card reader systems, biometrics, radio frequency ID and optical character recognition devices. And we can use data from those devices to manage the video."

Denari intends to use these capabilities to create a catalog of anomalous conditions that the video system will catch and bring to the attention of security.

"We want real time video alarms to assess and evaluate," he says. "Then we can build comprehensive situational awareness throughout the airport."