



The New Standard in Drive-up Intercom Systems
 Audio Authority® 800-322-8346

Security Products



The Integrated Product Newsmagazine for Security, Fire & Safety Professionals

[SUBSCRIBE](#)

[MEDIA KIT](#)

[READER SERVICE](#)

[CONTACT](#)

The CCTV Evolution

CCTV surveillance continues to evolve as it begins to include intelligent video software

By Brooks McChesney

THE security industry is in the midst of the most dramatic evolution in the use of CCTV video surveillance cameras since these systems were first deployed almost 40 years ago. While advances in electronics have enabled smaller and increasingly reliable cameras and other hardware, the real breakthrough is in the way video can now be captured, recorded and analyzed.

Intelligent video software technology will propel the industry from an after-the-fact, capture and replay tool to a proactive asset that will enable responders to detect suspicious activities when and even before they occur.

Intelligent video means that intelligence is added to video as it is captured and analyzed by behavior recognition software. CCTV combined with intelligent video software generates more accurate alerts and alarms, and results in greater situational awareness of threatening situations as they unfold. With this new technology, security managers can better deploy their human resources, achieve significant savings in monitoring costs and have the satisfaction of knowing there is a blanket of protection across their entire CCTV network.

Intelligent video software is currently being implemented and tested by the Transportation Security Administration at various facilities in an effort to impact security levels as soon as possible in government and transportation facilities. The software also has a key role to play in defending critical infrastructure facilities, such as banks, data centers, utilities and power plants. As awareness of the demonstrated value of software-equipped CCTV continues to grow, intelligent video is rapidly evolving into a mainstream technology.

The Application of Behavior Recognition

A prime benefit of intelligent video is that it eliminates the need for continual human monitoring of video for possible incidents. The task of watching video monitors is complicated by the number of cameras and their rotation cycles, along with the numerous other responsibilities assigned to security personnel.

With intelligent video, no one needs to watch monitors on an ongoing basis. When a predefined behavior occurs, the recording begins automatically, and alarms and alerts are sent to responders. If a responder does not take action in a specific time period, the alert is sent to the next responder.

The software coordinates a comprehensive, enterprise-wide response. This is especially important when several different groups of responders are needed to interdict a specific event. Intelligent video also allows security personnel to go back and review individual responses to an incident, analyze the incident logs and response times, and implement improvements where necessary.

AltaVista
Babel Fish
 To translate this page
 click a flag!



[Print this Page](#)

Intelligent video software is currently being implemented and tested by the Transportation Security Administration at various facilities in an effort to impact security levels as soon as possible in government and transportation facilities.

[Click here](#) to email this page to a friend.

Sophisticated behavior recognition software available today can recognize a human being, distinguish him or her from an inanimate object and accurately determine the number of people in the camera view. Video algorithms can identify specific types or sizes of vehicles, packages or pieces of luggage, as well as a wide range of human behaviors and actions such as loitering or penetrating a secure area.

The Critical Need for Standards

As with any category of technology, reliable, agreed-upon methods to measure the accuracy and efficacy of intelligent video are needed to understand its value and enable informed comparisons in the marketplace.

Industry standards will help define what "accuracy" means in the context of intelligent video. For example, a system may be very accurate at what it does, but those things may be limited. A system may be able to track an object moving in a single direction with no clutter or environmental constraints, and indicate if the object is crossing a line such as a fence or perimeter. However, that does not automatically ensure that in a forest or rain storm, or with four people at the same time, that same system will continue to be accurate.

Standards are a critical issue, and TSA and the National Safe Skies Alliance, among other industry bodies and agencies, are involved in software testing that could be a foundation for accuracy benchmarks for security technology.

Recently, TSA announced criteria for biometric devices, citing guidelines for technology to be deployed in airports. When such criteria are established for intelligent video, they should include such elements as accuracy, breadth of detectable behaviors, conditions under which the system must operate to be truly effective and the ability to integrate with other devices. It also must reveal the number of cameras it can support.

These vital criteria, plus others that define the ability to generate alerts and manage the required responses, will help purchasers make informed decisions and ensure that security needs are met.

To use behavior recognition technology, the first step is to identify the precise problem or threat at the location, then select the appropriate algorithm that matches that behavior type. Libraries of algorithms are being expanded and created to serve highly specialized surveillance requirements.

By freeing security personnel from the tedium of watching multiple camera views when no activity is occurring, intelligent video enables them to react only to those events that need immediate attention and action.

The Value of Pattern Recognition

The infrastructure for intelligent video already exists; the cameras, cabling and recording devices already are in place. The challenge is managing these numerous cameras and their views.

To achieve maximum effectiveness, the software must be deployed on multiple cameras across a building or facility. This enables proactive pattern recognition that cannot be achieved via a single camera. With pattern recognition, accuracy is achieved not only in terms of recognizing events as they occur, but more importantly, in having the ability to anticipate a threat before it is carried out.

For example, if people are repeatedly observed taking pictures of a facility, or the same people make frequent visits, such an activity could point toward surveillance or simulations enacted for purposes of an attack. This type of detected behavior realized at multiple facilities would automatically precipitate an investigation and enable proper authorities to take decisive action to interdict the threat before an incident occurs.

Pattern recognition is a strength unique to software. A simple example is a security guard watching a perimeter at an airport or high-rise office building. A car is parked along the fence on a Monday morning, but unless the guard investigates, it's unknown whether this is an employee on break,

[Ads by Goooooogle](#)

[CCTV DVR Internet Viewing](#)

Large Selection of DVR's. View Cameras from Anywhere over Internet
www.cctvspecialty.com

[Digital Video Recorders](#)

Mobile, Small, Medium, Enterprise For Intelligent CCTV Security
www.marchnetworks.com

[32 Camera CCTV DVR](#)

Combines cameras from all servers View Live Web Demo Now
www.video-insight.com

[Surveillance](#)

ADT® Video Surveillance Can Help Protect Your Business. Learn How!
www.ADT.com

[Advertise on this site](#)

someone watching airplanes take off or a suspicious vehicle. If the same car appears at a different place along the fence on a Wednesday, the same guard may not be on duty, or he or she may not remember it. Even more significant, if the same car appears at the perimeter at other airports in the region, it is improbable that humans would be able to connect the incidents.

Software is ideal at identifying such a connection as a pattern emerges. Software can raise the attention of security personnel, who can then investigate the matter in person and respond in an expeditious manner. In this way, the software frees the guards of the need to spend valuable time watching camera screens when no activity is occurring; it enables them to react proactively when a suspicious event is detected.

The Importance of Multiple Inputs

Ultimately, success with intelligent video is about receiving and integrating as many inputs as possible. This is why integration with access control is valuable in a facility concerned with unauthorized entry. If an ID card is denied at one portal and the system detects another ID denial at an adjacent door, followed by a tailgating incident, the "dots" are automatically connected to reveal a serious breach that may be occurring.

The more data points that can be observed, the clearer the pattern becomes. Once a pattern is detected, security personnel can analyze it and take action.

Video is a central element for pattern detection, but is not the only source of valuable input. Results from standalone sensors such as smoke detectors, biometrics and card readers can be stitched into the framework of video to provide "video plus" awareness. Security personnel can look at a video and see data about the person whose card caused the door to open, for example.

In this way, integration of many inputs into a common data file makes the video more complete, helping responders quickly see the whole picture of what is occurring.

Looking Ahead

With advanced intelligent video software bringing behavior recognition and alert management technology to CCTV systems, security capabilities are being extended in ways that were not possible a few years ago. Security personnel can do their jobs more effectively, and security resources can be deployed in more cost-effective ways.

As the quality of optics improves, and CCTV systems begin to include high-definition cameras, as well as thermal and infrared devices, there will be a dramatic leap forward. Other developments are likely to include the placement of software intelligence at the camera itself, so that video files are transmitted over high-bandwidth networks only when they contain useful information.

As standards are established and intelligent video technologies continue to evolve, security personnel will be able to anticipate and respond to events even more rapidly, effectively and efficiently.

This article originally appeared in the January 2006 issue of *Security Products*, pg. 28.

Brooks McChesney is president and CEO of Vidient Systems Inc.



[Search](#) | [Subscribe](#) | [Free Newsletter](#) | [Free Product Info](#) | [Advertising](#) | [Contact Us](#)

© Copyright 2006 **Stevens Publishing Corporation**

5151 Beltline Road, 10th Floor, Dallas, Texas 75254

Reproduction in whole or in part in any form or medium without express permission of Stevens Publishing Corporation is prohibited.

[Privacy Policy](#) | [Reprints](#)

Contact the [webmaster](#)