International Council For Industrial Security & Safety Management

Newsletter: May 2016

Many in the security industry are aware that intelligent video is a mainstay of heavyweight security installations that can well afford top-end security technology. This perception has spread throughout the security industry where intelligent video is viewed as the crown-jewel of big-budget security programs, such as airports, military, and nuclear power sites.

Early intelligent video developers share some of the responsibility for this exclusive upscale security perception in part because they focused on working solutions that were rather complex and expensive to deploy instead of paying attention to points such as easy installation and usability that would make intelligent video viable for common security installations.

Today's commercially available intelligent video systems are breaking new ground to deliver high-performance and proof-positive detection, yet in a simple to install and operate intelligent video edge device or all-in-one camera. Commonly, industrial security administrators are finding themselves overwhelmed by new trends in crime and added responsibilities of security conformance issues. Often they are bogged down with traditional security devices and antiquated operational procedures that are part of timeworn security programs.

Despite the drawbacks of traditional security measures, the fresh demands of industrial security, and the advantages of intelligent video to fill this void, security integrators fell behind in deploying these more effective solutions over the traditional devices they know and love. In the near future, security installers will begin to find greater demand for intelligent video solutions, especially for the industrial security marketplace where benefits and the return on investment on of intelligent video solutions are sizable.

With very best regards

Capt S B Tyagi

International Council For Industrial Security And Safety Management

Intelligent Video Surveillance

Security with Heart & Brains

Changing criminal trends are putting security under pressure as they try to cope with problems, such as shooting rampages, terrorism, scrap metal theft, industrial plant theft, and frivolous injury claims. After critical review, industrial security administrators discovered they have many security holes due to the fact that the run-of-the-mill security components used for industrial security were never designed for wide area detection or anti-terrorism efforts. The surveillance technologies were also unable to foresee or forecast the treats as logical analysis and trend projections were not possible with the available technologies.

Security risks not previously believed to be at issue, including theft of hazardous chemicals, medical waste, and combustible materials present new threats and challenges for industrial security programs to overcome. Formidable areas that are problematic or unpleasant to patrol yet provide access to crazed intruders such as hazardous confined spaces, high-voltage areas and hazmat facilities now need to be secured. With tight budgets and a tendency to shy away from new solutions, industrial security remained unable to secure perilous, inhospitable, and wide-open areas.

Business intelligence solutions have revolutionised the enterprise, converting a relentless deluge of data into actionable information that can shape strategies, improve processes and boost bottom lines. The core benefit of such solutions is compelling: maximise the value of raw (unstructured) data through rigorous analysis that reveals key trends and correlations hidden within that data.

With the advent of surveillance digital video recorder (SDVR) systems, security professionals now face a similar challenge. While SDVRs and IP-based network DVRs (NDVRs) enable unprecedented access to vast quantities of high-resolution video

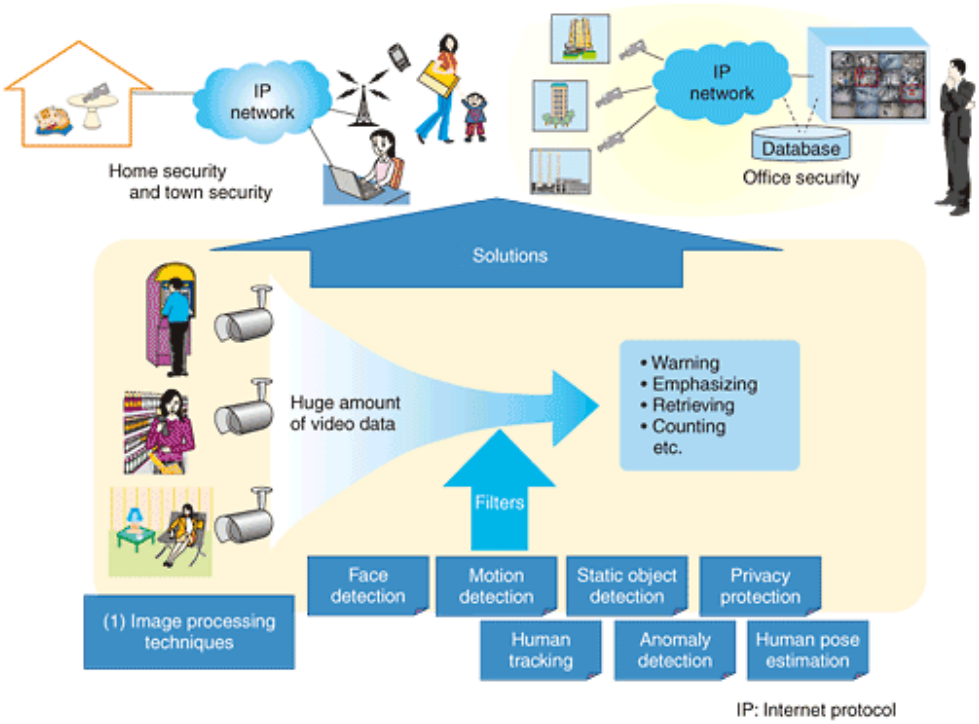
images, deriving maximum benefit from this wealth of raw surveillance data requires meticulous review and analysis, sometimes on a frame-by-frame basis.

The intelligent video benefits are many. Areas those are too inhospitable for guards to regularly patrol can be automatically watched over from remote. The capability of monitoring wide areas and detect not just short-range movements such as an infrared motion detector, but true intruder behaviour scenarios, allows intelligent video to cover security holes. The unique ability of intelligent video detection to differentiation between persons and trivial small animal movement allows it to outperform primitive sensors and detectors that typically alarm on any spurious movements.

Fact is security guards cannot be everywhere at once which translates into missed opportunities. All too frequently, guards discover incidents after the intruder has caused the premises and committed a crime, after the burglar has run away with valuables, and after the damage is done. With autonomous intelligent video monitoring, security officers are alerted within seconds rather than waiting for scheduled patrols to stumble upon an incident or a concerned passer-by to report it.

An intelligent video edge device - DSP-based devices with self-sustained video analytics provides industrial security administrators with a plug-and-play solution that is easy to use and install. It also is ideal when a remote or stand-alone deployment is needed for any application, such as remote construction sites, electrical substations, agricultural sensors, school campus perimeters, and pipeline infrastructures where it can work without a dedicated network processing computer or onsite security guard. In addition, intelligent video offers a viable and easy to install solution as an invisible fence that can provide an early-detection advantage and a cost effective alternative rather than erecting truckloads of fencing, fence sensors, ground sensors, and wiring that can often include battles with zoning and local residents about aesthetics of the security fence. Intelligent video provides industrial security the ability to magnify capabilities, reduce resource utilization, and broaden security coverage so that security programs can overcome modern security challenges.

- Intelligent video detection can distinguish between vehicles and people and even limit detection to a specific direction, so when an unauthorized intruder wanders on the property it will be detected, but an employee vehicle leaving the work would be ignored.
- Automatic detection of object removal can be used to limit detection to items that are of interest whether it is the taking of



a loading-dock computer or a palate of copper piping from a storage yard.

- Automatic detection of unattended objects can reveal when a box of products is tossed over the fence by an employee for after work plunder or alarm when a suspicious package is placed next to liquid propane tanks.
- Automatic detection of stopped cars can notify when a vehicle parks outside at a strange hour or when a suspicious (possibly explosive-laden) car parks nearby chemical storage tanks.
- Autonomous pan tilt zoom tracking, unlike stationary cameras, can provide automatic close-ups of an identified moving target for better security-usable images or to provide real-time tracking of a camouflaged intruder whereabouts.

With intelligent video edge device interfacing and event engines, lights can be turned on, barriers raised, doors locked, and warnings announced automatically on an alarm event. Additionally, scheduling of different detection criteria can allow industrial security to narrow detection on items of interest. For example detection can be scheduled for late night or shift change scenarios, as well as PTZ camera tours with different detection on each pre-set. Also in the intelligent video offerings is advanced synchronized handoff of moving intruders from stationary camera detection to autonomous PTZ cameras for robot-like tracking.

Beyond reducing labour expenses and providing a cost-saving security alternative, intelligent video offers significant returns that make deployment highly attractive: security personnel become more accountable for all alarms, instant automatic notification, recording and deterrent messages/actions (ideal for prohibited entry into controlled or hazardous areas) as well as helps meet security conformance in order to avoid noncompliance citations and negative publicity. Providing remote analysis capabilities and PTZ tracking for informed response and constant visuals on intruders, the intelligent video detection helps increases scene safety for responders.

Remote Video Response Centre

CCTV monitoring via a Remote Video Response Centre (RVRC) is an area of security that operates steadily in the background. In recent times, it has become one of the key driving forces behind improved practices and standards. Mark Thomas offers end users his thoughts on the current status of remote site monitoring, new technologies and what the future might look like.

There are two types of CCTV monitoring:

- Reactive monitoring involves alarm detection on site which initiates a picture transmission to the monitoring centre who use this for visual confirmation and deal with it appropriately
- Proactive monitoring (city centres and high street locations, for example) takes place in real time. An operator constantly reviews the location and is able to immediately alert the appropriate security or emergency service of an incident

Both types of monitoring provide recorded evidence of events and these recordings are frequently used by police to assist with their enquiries; they also help the police to build cases by supplementing non-related incidents.

Comprehensive CCTV monitoring is made up of three constituent parts the security equipment installed on site, the monitoring facility (or Remote Video Response Centre) and the transmission equipment that enables live video and audio communication between the two. It's worth exploring each of these areas in relation to how they can provide the end user with an effective, end-to-end security monitoring system. Despite the conflicting demands of what is predominantly a price-driven market, it will become apparent that quality is demanded throughout.

Let's first look at the current standards for CCTV monitoring. British Standard 8418: Installation and Remote Monitoring of Detector-Activated CCTV Systems (Code of Practice) was designed to ensure a minimum level of operation across the entire monitoring service. As you'd expect, then, it provides essential design, installation, commissioning and operational guidelines for those involved with remotely-monitored CCTV, and is looking to 'raise the bar'.

Significantly, BS 8418 enjoys total endorsement from the Association of Chief Police Officers (ACPO) in recognition of the fact that it will help to drastically reduce false alarms and prevent unnecessary police call-outs. As such, ACPO has extended the issuance of Unique Reference Numbers (URNs) – previously only issued to intruder alarm system installations to include detector-activated CCTV systems that are BS 8418-compliant.

It's fair to say that the effectiveness of a CCTV installation depends on the equipment used and the quality of the installation itself.

Proof in the real world

Most solutions providers promote their wares to end users on the grounds of complex functionality. Purchasers would be well advised to gather data on a given product's ability to deliver that functionality in the real world both as a system in its own right and during operation using BS 8418 as the benchmark.

The quality and intelligence behind an end-to-end system will dramatically influence its effectiveness. Only those installers who are NACOSS (or National Security Inspectorate)- approved should be employed by the end user. These approvals indicate procedural compliance and that an agreed audit trail will be followed. They demonstrate a willingness to be registered and inspected, and commitment to a high quality installation service. However, those same approvals are still not confirmation that the systems designed and installed will function and operate with false alarm reduction or effective off-site monitoring as their goal. In the future, we need to be demanding a BS 8418 accreditation for installers, thus ensuring they are sufficiently well trained and competent in their role. This must also extend to accrediting the CCTV systems they provide.

When it comes to selling a CCTV system, there's likely to be a cost increase for a BS 8418 system. That said, the end user redeems that cost over time through reduced false alarms, lower numbers of

police call-outs and, ultimately, improved crime prevention. If a system isn't BS 8418 compliant, the URN necessary for police response can only be granted for the intruder alarm element of the site security system. The CCTV system is then only used to visually verify the alarm.

'Soak' test before 'going live'

A useful, independent means of assessing a CCTV installation would be to invite the chosen RVRC monitoring station to carry out a 'soak' test before the system goes live. This will highlight any system inadequacies and demonstrate whether or not it's likely to elicit false alarms. The RVRC's engagement team could also provide a list of recommendations necessary for solving on-site problems and improving system effectiveness. It's up to the end user to decide whether they choose to follow those recommendations, but time and money will usually be saved if attention is paid.

The RVRC management team can always refuse to monitor a site if the on-site security system is deemed inadequate, and would use up too much valuable operator time. Not a popular choice for them, as they'd lose a potential customer. Again, BS 8418 may be deployed to insist on minimum site standards.

Choosing a Remote Video Response Centre is much easier than selecting and installing a CCTV system. RVRCs can be BS 8418-accredited. Indeed, the benefits of selecting a compliant Centre are very significant. BS 8418-approved stations boast specifically-trained, Security Industry Authority (SIA)-licensed operators. The RVRC has to provide 24/7 monitoring, and boast a comprehensive back-up system in case of network or power failure.

In addition, a BS 8418 RVRC will have specific procedures in place for handling incidents, logging the outcomes, calling the police and informing the client. The levels of service demanded are difficult and challenging to provide, requiring a high standard of operation. This often comes at an increased cost to the user, but the payback will always prove positive.

Qualities of Remote Video Response Centre

1. A fast alarm response rate: A monitoring station should always respond to alarms quickly. To be compliant with the British Security Industry Association, specifically the British Standard BS8418, an alarm-receiving centre must respond to alarms in under 90 seconds, at least 80% of the time. Responding to an alarm quickly means that the cause can be identified and a remedy put into action as soon as possible. This will reduce the impact of damage caused, and if necessary the police can be contacted.

2. Site security experience

A remote video response centre should have experience in providing the type of services you're looking for – and in setting up an installation for similar sites. Responding effectively to alarms relies upon the skills and trained judgment of the people behind the cameras. This often depends upon their experience, confidence and knowledge of the type of site they are monitoring. Ask your chosen remote video response centre for the number of sites they monitor, which are similar to yours.

3. Transparency and trustworthiness: It's essential that you trust the quality of service you're receiving from a monitoring station. For that trust to happen, you'll need to understand how the remote video response centre works. They should happily supply you with the following information:

The amount of alarms from your site, and when they happened; Who dealt with each alarm and what action they decided to take; How quickly they answered each alarm; How they dealt with the discovery of any equipment or communication problems, And a real-time update of the connection between your site and them, as well as an agreed procedure for letting you know about the loss of a connection.

4. Customer service: You will have questions about your security system, particularly whilst it's new and the installation is taking place. Look for a remote video response centre that has personnel dedicated to ongoing liaison with customers. This is not only essential for answering your questions but also for keeping information and contact details up-to-date, so you can be notified quickly when necessary.

5. A Great alarm to operator ratio: The more operators there are available to answer alarms, the more time they will be able to spend finding the cause of alarms. When an alarm goes off, you want a dedicated team member to quickly and diligently find the cause of that alarm. Ask your chosen remote video response centre for the number of operators on shift, and the total number of alarms they can expect to receive on that shift.

6. Confident and effective handling of alarms: To make sure the cause of an alarm is properly assessed the operator should be looking at different images taken when the alarm was first raised. The initial alarm image may not show the cause of the alarm, so dismissing it without looking at further images could mean an incident is missed and not acted upon.

New Video Analytics: Tools for Efficiency

Video Analytics or Video Content Analysis Software (VCA) is the capability of automatically analyzing video to detect and determine temporal and spatial events. This technical capability is used in a wide range of domains including entertainment, health-care, retail, automotive, transport, home automation, safety and security. The algorithms can be implemented as software on general purpose machines, or as hardware in specialized video processing units.

Many different functionalities can be implemented in VCA. Video Motion Detection is one of the simpler forms where motion is detected with regard to a fixed background scene. More advanced

functionalities include video tracking, head-counting, fall detection, traffic direction rule enforcement and 'egomotion' estimation.

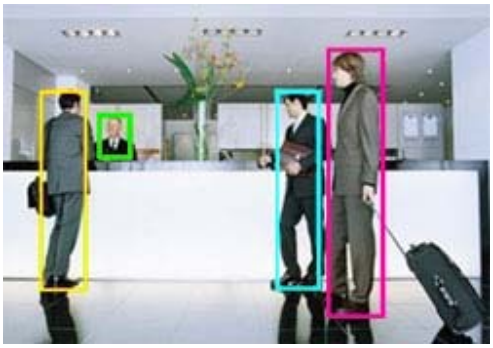
Based on the internal representation that VCA generates in the machine, it is possible to build other functionalities, such as identification, behavior analysis or other forms of situation awareness. VCA relies on good input video, so it is often combined with video enhancement technologies such as video denoising, image stabilization, unsharp masking and super-resolution.

Police and forensic scientists analyse CCTV video when investigating criminal activity. Police use software which performs video content analysis to search for key events in video and find suspects. Surveys have shown that up to 75% of cases involve CCTV. Police use video content analysis software to search long videos for important events.

Though biometric analytics have been around for a few years now, Apple and Samsung's recent introduction of fingerprint readers to their newest mobile devices prove that biometric security systems are going to be more and more commonplace in the public sector. The research organization Goode Intelligence estimates that biometric authentication will be on most mobile devices by the end of 2015 and that by 2019, it will be used by 5.5 billion people worldwide. Familiarity with biometric analytics means ease of use for employees and consumers alike.

Surveillance and ports seem to go hand in hand – travelers hardly notice the myriad security cameras in airport terminals, and ferry passengers are similarly unsurprised when their transportation and loading areas are markedly under surveillance. However, not all surveillance cameras, systems or even analytics are fit for port security, as Steve Vandor soon discovered.

Vandor is the deputy director of IT for the Washington Department of Transportation, Ferries Division – including the largest ferry system in the United States, the Washington State Ferries. In 2010, the existing surveillance system was becoming obsolete, both from aging equipment and a looming lack of support from the manufacturer. In 2011, the state-run entity began implementing a new system with G4S Technology.



"A lot of events, by themselves, are innocuous. For example, a boy and his father are poking about the docks, where people normally aren't going, because they're mad about boats. That shouldn't alert security. But a person, at night, in a hood or balaclava, that should trigger an alert. Our challenge lies in how we can deliver these parameters," he adds. Constructing these rules "is the highest kind of service that IT can provide security."

According to Greg DeCanio, the Chief of Law Enforcement at LIMA, the new video management system provides airport security personnel with "the ability to access video at our computers, making us more efficient and letting us monitor activity for security and law enforcement purposes at the touch of a button."

"The quality of the HD video with the panning and zooming features of the cameras have been so helpful in our security efforts," he says. "There have been multiple cases when we have needed to go to the video archives and IPVideo's solution has assisted us in successfully completing investigations. We have been able to go back to these archives and quickly find what was needed. The system has made our lives easier and, most importantly, more secure for all who travel through and operate in our airport."

Officers can use the new HD cameras to capture facial details and aid officers in identifying persons of interest and resolving incidents. They can also use the system to improve overall customer service by quickly reviewing video to help travelers find lost property and locate cars in the parking lot.

Ray Davalos, the Building Systems Manager at Miami International Airport, is also using technology to support, not replace, his staff. PSIM (Physical Security Information Management) and other software help the airport's security team mitigate any internal threats.

"Our top priorities are instantaneous sharing of information between security stakeholders through the use of a consolidated system," he says. "We require all parties to share relevant information at a moment's notice. … We can leverage on-site staff and tenants as vigilant eyes and ears to detect anything out of the norm. They are trained in behavior pattern recognition and can report any threat via their smartphone to a security Web portal. The system analyzes this big data and reports to the proper stakeholder for investigation."

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

---

Suggestions & feedback may be sent to us on e-mail: onlineicissm@gmail.com

---

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list. Thank you!

Forthcoming Events

BASIS 2016: Smart Security – The Doors to the Future

GDSF Annual Seminar: