



# International Institute of Security & Safety Management



*Let's professionalize the professionals...*



## Newsletter of NCR Chapter : April 2009



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.

**Capt S B Tyagi, FISM, CSC  
For NCR Chapter, IISSM**



## Covering New Ground - Intelligent Video Surveillance



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.

Security risks not previously believed to be at issue, including theft of hazardous chemicals, medical waste, and combustible materials, present new 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.

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 behavior 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 cased 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 passerby 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 pallet 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 preset. 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 labor 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 non-compliance citations and negative publicity. Providing remote analysis capabilities and PTZ tracking for informed response and constant visuals on intruders, the intelligent video detection helps increase 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.

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 management 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.

---

## **New Technologies Improve Building Security Design**

While building developers are increasingly being asked to analyze and improve building security, developing technologies assisting engineers in the pursuit of safe working environments couldn't have better timing.

Building owners and developers have increased interest in the security plans of the new structures since the events of 9/11. The first step they need to take is to analyze the potential threat of a building. Vulnerability and threat assessments study everything as a system rather than just what can be done to protect. Risk assessments determine how much security is really needed.

The U.S. Army Corps' Construction and Engineering Research Laboratory in Champaign, IL, is working on software to help architects understand potential threats. This tool will aid them in



designing buildings with a certain threshold of protection. The software will help the architects evaluate complicated issues such as computational fluid dynamics, without having to know what that is. The software will familiarize designers with different materials. For example, engineers will learn about high-tech carpets that can neutralize contaminants and other characteristics of particular materials in regards to security.

By creating dynamic models, the Corps is able to look at the water treatment of an infrastructure. These models will help officials identify access points to the water system, and to evaluate water towers, manholes, well heads and fire hydrants. All of these points are considered vulnerable in a water system, although they are not usually well-secured.

The Metropolitan Water District of Southern California (MWD), a public utility, is not waiting for the government directives. It will purchase contaminant monitoring equipment and instrumentation and upgrade its analytical capabilities and automated, remote water-quality sampling. In addition, it will also increase security at water filtration plants.

Chlorination and dilution are both effective ways to prevent water contamination. The fact that U.S. systems still chlorinate water to disinfect it is a great advantage. Super chlorinating is an inexpensive killer of bioactivity. Dilution is another way to prevent chemical contamination. According to Ed Wetzel, Vice President of Montgomery Watson Harza, Pasadena, CA, "It is difficult to add enough of chemical contamination to be a threat."

Sandia Laboratory, the U.S. Dept. of Energy in New Mexico, has developed a risk assessment methodology for dams, transmission and water systems. As a tool to assess vulnerability, Congress may require the use of this method for all public agencies.

The American Society of Heating, Refrigerating and Air-Conditioning Engineers Inc., Atlanta, GA, recommends owners should become familiar with their safety systems. While solving one problem, building owners are warned to consider they may be creating another problem. Street-level intakes might be replaced with roof air intakes, but they are not intruder-proof and must be secured against biohazards and guarded. Closing off air intakes can reduce a system's ability to purge contaminants. Also, they should consult local fire marshals when considering blocking ventilation paths or changing the designed airflow patterns.

ASHRAE suggests shell and duct tightness, areas of refuge, and fire protection and safety for the entire building all need to be studied, not just heating, ventilating, and air conditioning. Lower-risk buildings can install stand-alone HVAC systems or simply move the mailroom or other "high-risk" functions off-site for affordable protection. Expensive high-efficiency particle air (HEPA) filters in HVAC systems will filter out particles down to 0.3 microns but pre-filters can be installed leaving HEPA filters as a final filtration system.

A final way to reduce risk is to deter. If the intruders to the structure can be slowed down enough, then the response teams will have the opportunity to catch the intruders before anything harmful can be done.

**"Pity the meek, for they shall inherit the earth!" - Don Marquis**



# Feedback

There were rather two very interesting feedback received on the contents of our last Newsletter. Both the mails are reproduced – one is with positive feedback from the security professional with acknowledged credentials and other one is an outpouring of frustrated national of a failed country!

Kindly note that this 'indignant' citizen is not even writing the name of his country with capital P. So much for patriotism!

I still maintain that Pakistan is a 'failed' nation.

**- Capt S B Tyagi**

---

**From:** D.C. Nath [mailto:nathdc@iissm.com]  
**Sent:** Friday, February 20, 2009 6:06 PM  
**To:** Mark Schol  
**Cc:** Corporate Security Department; captsbtyagi@yahoo.co.in  
**Subject:** Re: Reaction on Newsletter of NCR Chapter of IISSM: Feb. 2009

Thank you, Mark Schol.

Your concern is very genuine and the apprehensions expressed are very real. Unfortunately, it is very difficult to convince the concerned about such up gradation of security business. We in the IISSM have been trying nevertheless.

'Shall welcome suggestions that can be implemented in practical terms under the Indian conditions.  
Best regards,

Yours sincerely,

**D.C. Nath**

Copy to: Capt. S.B. Tyagi.

----- Original Message -----

**From:** [Mark Schol](#)  
**To:** [Corporate Security Department](#) ; [captsbtyagi@yahoo.co.in](#)  
**Cc:** [nathdc@iissm.com](#) ; [premsagar@iissm.com](#)  
**Sent:** Thursday, February 12, 2009 9:36 PM  
**Subject:** Reaction on Newsletter of NCR Chapter of IISSM: Feb. 2009

Dear Capt. S B Tyagi,

I thank you very much for your email and news letter.

Unfortunately, it is impossible for me to attend the 12th India International Security Expo 2009 in New Delhi that will be held in 2 weeks time.

In the news letter you gave a perfect description of Mr. President of the USA Barak Osama, armored limousine. It needs to be explained that this is a B9/B10 type of armored limousine. Only the USA can armor this type of cars and they are only used for the President of the USA.



Traveling with armored private cars in India, still today seems more like an illusion. I still today see that government officials are driven around New Delhi in unarmored AMBASSADOR cars. There is no protection of any kind build in those cars. After the Mumbai attacks, the government should better protect their international officials, like ambassadors, and their own members of the Indian Government. My King, Albert II of Belgium, visited your country a few months ago. It was a mass media event to have the King of Belgium in India. During his visit in your country, I every day feared for his life. He was taken around the country, without any professional protection. This means no armored car (B7), no professional bodyguards (trained in Israel), no professional hotel protection measures, etc.

I fear that India is doing lots of talking but does not do any mayor investment on real security work. At the IISSM conference 2007, when I took the stand the last day of the conference, you will remember that I said the following things.

1. A terrorist attack of very great impact will strike India at any moment. You are not ready to counter that attack. Unfortunately it happened.
2. Multiply the salaries of the security agents with 1000. Make them the best paid staff in India. When they are well paid, it is very difficult to bribe them.
3. Increase the basic cost for private security services with 1000%. If people want to be safe, they will pay for it. Stop competing on being the cheapest.
4. I love India, it is as a second home to me, and I want this beautiful country that I love so much be safe for anyone.

ICLMP is representing a world wide renowned company for armoring cars. They mainly provide armored private cars for the Middle East. They can stretch and Armour B7 Mercedes S500; Rolce Royce; Bentley; Maybach; Land Rover etc. They can include full business packs.

ICLMP works together with the best security training schools in Israel for body guards, VIP protection, mass-protection; unarmed combat protection, etc.

It is time now that the people in India really get professional protection.

I hope that with this email, I did not offend you, or any of the members of the IISSM or any other person. I am sure that together ICLMP, the IISSM, all the members; we can make India the safest place in the world.

Looking forward to hear from you in the very near future, I remain,

**With kindest regards**

**Mark R. Schol**  
**International Director**

*International Coordination in Logistics for Management Programs - ICLMP*



**Mobile** : +32 (0)477 632504  
**Phone** : +32 (0)3 6375960  
**E-mail** : [ms@iclm.com](mailto:ms@iclm.com)  
**URL** : [www.iclm.com](http://www.iclm.com)  
**Skype** : iclm.mark



**Advisor for Security, Safety, and Prevention.**



**From:** Tashfeen Baig [mailto:tashfeenbaig@hotmail.com]  
**Sent:** Monday, March 09, 2009 12:10 AM  
**To:**  
**Subject:** RE: Newsletter of NCR Chapter of ISSM: March 2009

*Tyagi,*

*I am not surprised why you were retired or may be thrown out of the army as a captain, that your thinking is so myopic, what kind of a security professional are you who cannot rise out of India. You have the guts to send an e mail calling pakistan a failed state, a rogue nation, the mail which is also addressed to some of us in pakistan, you should be ashamed of yourself, For the sake of your cheap popularity & that of the newsletter, desist from cheap talk...you will not become an Indian hero through cheap means, DO something worthwhile!! You are not a politician. Learn to chew in private. In all fairness you owe an apology to all security professionals...Let us rise above... differences may remain  
Tashfeen Baig, TI (M), CAS, CMAS*

## International Mobile Equipment Identity

This number has become frequent in the newsprint and media due to government's ban on cheap Chinese mobile phones which do not have these numbers. These phones are security hazards is another case. But what IMIE is?

It is a unique 15-digit code used to identify an individual GSM mobile telephone to a mobile network. It can be displayed on most phones by dialing **\*#06#**. It is also usually printed on the compliance plate under the battery.

Prior to April 1st 2004 the numerical format of the code was: 11111-22-333333-4

TAC						FAC		SNR					CD	
D14	D13	D12	D11	D10	D09	D08	D07	D06	D05	D04	D03	D02	D01	

- TAC: Type Approval Code
- FAC: Final Assembly Code
- SNR: Serial Number
- CD: Check Digit

The first six digits are the TAC (Type Approval Code), which identifies the country where type approval was sought for the phone, as well as the approval number. NOTE: since the 1st April 2004 the TAC will be the abbreviation for Type Allocation Code.

The FAC (Final Assembly Code) identifies the company that produced the mobile phone (e.g. Sony Ericsson or Nokia). NOTE: From 1st January 2003 a new code allocation procedure has been in place. The changes relate to the format - the Final Assembly Code (FAC) is obsolete and is set to 00 for the period from 1st January 2003 until 1st April 2004. The FAC is now obsolete, and the TAC is now eight instead of six digits, as follows: 11111111-222222-3

TAC								SNR					CD	
D14	D13	D12	D11	D10	D09	D08	D07	D06	D05	D04	D03	D02	D01	

The 6 digit SNR (Serial Number) has been uniquely assigned to the specific type of handset. The CD (Check Digit) is used to check the code for its validity for Phase 2 and Phase 2+ handsets. Phase 1 GSM handsets, however, always have zero ("0") as check digit.



# From the desk of Executive President & CEO



## Subject: Invitation for Papers for IISSM-2009.

As you would have noted, IISSM-2009, the XIXth in the series of IISSM's Annual International Seminars, is scheduled in New Delhi India, on December 9-11, 2009. The venue would be Scope Complex, Lodhi Road, New Delhi-110003.

In the context of the prevailing security scenario in South Asia in particular and in the world at large, it has been decided to have the theme for this year's Seminar as "**Role of Private Sector in Counter-Terrorism**". It is realized that private sector institutions and agencies can and should play a vital role in supplementing governmental agencies' efforts in this direction. As a matter of fact, after some guidelines indicated by the Union Home Secretary, Government of India, at IISSM-2007, we have, after consultation with some security professionals in the field, already gone up with some suggestions in this regard. But we now look forward to eliciting more specific thoughts, covering multiple areas, such as overall security management system, coordinated efforts by Private Sector Chambers/Associations, technology and systems integration, information/cyber security, aviation security, transport security, mega city security management, mall/multiplex security, possibilities of international cooperation in the areas of security and crisis management, expertise/equipment etc. After some select papers being presented by experts like you, it is proposed to throw open the subjects for more in-depth discussion during floor participation by the delegates.

May I, in this context, request you to kindly ponder over the matter and consider presenting a suitable paper at IISSM-2009, covering some aspect/s of the broad theme? Except in panel discussions, one hour's time is kept for a subject, with 40 minutes at the most for the speaker and the remaining 20 minutes for floor participation and other formalities. It will be highly appreciated if your presentation could include reference to actual case studies, as demanded by the participants.

IISSM being an academic organization, a convention has developed that we pay only one-night accommodation to the faculty but offer other local hospitality for all the days of the Seminar, including airport pick-up and drop-back. Well, we are obliged to all those who have been joining us year after year within these limitations.

We shall indeed be grateful to hear from you early. We wish to proceed along the following time-frame for this:

- **Expression of your interest to join as faculty: By May 31, 2009.**
- **Title of the paper you wish to present with an abstract of it within 200 words for the consideration of the Screening Committee: By July 31, 2009.**
- **The full text, on acceptance, of the paper: By October 31, 2009.**

Email communication is preferred for the sake of avoiding mistakes in transmission.

Thanking you in anticipation and with best regards,

Yours sincerely,

**D.C. Nath**

