Security Trends 2013
Product & installation highlights of 2012
The behaviour of cars
Be VIGILANT™
World Leader in Integrated Video Management Platforms

CCTV • Access Control • Offsite monitoring

UTM Group
converged risk solutions

0860222266  info@utmgrouplcoza  www.utmgrouplcoza
Features

Opinion
Industry experts comment on aspects of the security market pertinent to all players in the business.
- The behaviour of cars
- Someone’s watching me
- A real security solution
- Successful security contracts

Installation highlights 2012
SmartProtect integration software takes off
Android platform-based biometric reader
Smooth exit and entry at upmarket estate
Flexible real-time system for a Massmart chain company
You can bank on this solution

Product Highlights 2012

Vertical focus: Residential/estate security
Vertical focus: Security in education

Trends 2013

On the cover

ZKTeco: new name, new opportunities
ZKSoftware is well known in South and southern Africa as a supplier of access control and T&A products, both card and biometric based. This successful Chinese company has carved a significant share of the local market since it first launched its local operation in 2005. Hendrik Combrinck, who together with his team has made the company a household name in the access control and T&A industry over the past several years, heads the local office since 2009. See more on page 22.
EDITOR’S COMMENT

That thing that used to be called privacy

If you use Facebook, you might have seen a spate of status updates claiming that the user’s posts are copyright and can’t be used by Facebook (or anyone) without the account holder’s written permission. Of course this is useless as when you sign onto Facebook you sign away all rights to privacy and all those nice things so that Facebook can use whatever it wants from your profile to try to make money. Simply putting a new declaration on your status doesn’t change the terms of Facebook’s service, which it changes whenever it feels like it to benefit itself.

The issue is, of course, more than simply a matter of what Facebook does with your data (which is not private, no matter what you may think). It’s a matter of privacy in general and the erosion of it specifically. The worst offenders are not the social media sites that collect all your information, but those individuals who fill out whatever information the screen in front of them asks for without thinking, and then continue to update the site (and other social media sites) with details of every aspect of their lives. Being cool can be dangerous.

The best example of how careless people are can be seen in this YouTube video (http://www.youtube.com/watch?feature=player_embedded&v=F7pYHN9IC9I). It’s an advert from a bank in Europe. This clip has been seen by over 6 million people, but I wonder how many people actually pay attention to it. If you’re the type of person who puts personal information on social media, and in this case Facebook specifically – things like pictures of your kids – you should go to www.takethislollipop.com (I had trouble running it in Chrome, but it works well on Internet Explorer). The site was introduced at the launch of the 2012/13 South African Cyber Threat Barometer. It simply takes random information from your Facebook profile and incorporates them into a story. You have to sign in via your Facebook details, but it is safe, if not somewhat traumatic.

To practice good online behaviour, simply go to Facebook’s Privacy Settings, click on the “Ads, Apps and Websites” option and remove www.takethislollipop.com to revoke its access to your Facebook data – after you have watched it.

Of course, this is fun to watch, but it shows Facebook fans just how much information they are putting out there. So, how much of your life is online? And given the environment we live in, perhaps the more important question is, how much of your kids’ lives are online?

Andrew Seldon – Editor

LETTERS TO THE EDITOR

Letters to the Editor should be addressed to Andrew Seldon at andrew@technews.co.za. Sending material to this publication will be considered automatic permission to use in full or in part in our Letters column. Be sure to include your name, e-mail address, city and postal code. We reserve the right to edit all letters.
I walk in the customers shoes, understand the whole picture and persist to overcome challenges

I am dynamic vision and these are my cameras

Christopher H
Applications Engineering Manager

I hear it every day from customers. Why should I move to IP when I have invested so much in analogue cameras? My challenge is to show you how the power of American Dynamics can help your systems run better, smarter and faster. That is my dynamic vision and these are my cameras.

My dynamic vision - Your solution

The Illustra 600 IP Series HD Mini-Domes deliver clear high-definition video at full frame rates of 25ips. So whether in bright sun or near darkness, you can clearly see important details such as superior facial detection, something that is rapidly growing in importance in education, healthcare, and retail applications. Configuration is also simplified using the Illustra Connect tool. Add to this onboard motion-detection, and advanced integrated analytics, all of which reduce your ongoing cost of operation by minimising the cost of storage while ensuring HD image quality. All of this over your PoE and PoE+ network.

American Dynamics
A Tyco International Company
## CALENDAR OF EVENTS

### EVENTS, CONFERENCE, SPECIALISED EVENTS, WEBINARS

<table>
<thead>
<tr>
<th>Event</th>
<th>Dates</th>
<th>Location</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mining IQ in partnership with the Security Association of South Africa (SASA) is hosting a Mine Site Security Africa Conference. It will offer a platform for mining professionals to benchmark their work in corporate security.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IFSEC West Africa</td>
<td>5 – 6 March 2013</td>
<td>Lagos, Nigeria</td>
<td>Specialised Exhibitions Montgomery, +27 (0)11 835 1565, <a href="http://www.ifsecwestafrica.com">www.ifsecwestafrica.com</a></td>
</tr>
<tr>
<td>The 2013 show will include the launch of a dedicated Safety Pavilion, aimed at exhibitors specialising in occupational safety and health (OSH).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecurExpo 2013 (Zimbabwe)</td>
<td>13 – 16 March 2013</td>
<td>Harare, Zimbabwe</td>
<td>Conrad Chibanda, Mobile : 00 263 775504180 / 00 263 773 836306</td>
</tr>
<tr>
<td>The SecurExpo 2013 event will be running on the theme “Integrated Security, providing Global Protection” reflecting the integration of security solutions with global innovations in one package.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copper Cable Theft Conference</td>
<td>8 – 11 April 2013</td>
<td><a href="http://www.iir.co.za/index.php/copper-cable-theft-jhb-conf">www.iir.co.za/index.php/copper-cable-theft-jhb-conf</a></td>
<td>This second annual conference will provide an update on the latest strategies to combat copper theft and will look at the latest technologies to protect copper cables.</td>
</tr>
<tr>
<td>Secutech 2013</td>
<td>24 – 26 April 2013</td>
<td>Taipei Nangang Exhibition Center in Taiwan</td>
<td>Ms Lois Lee 886 2 2659 9080 ext 358, or <a href="mailto:lois.lee@newera.messefrankfurt.com">lois.lee@newera.messefrankfurt.com</a>, <a href="http://www.secutech.com">www.secutech.com</a></td>
</tr>
<tr>
<td>Secutech 2013 is the 16th edition of the show, a business platform for global security professionals to find new business opportunities as well as enhance their brand reputation. The show is expected to attract 560 exhibitors and welcome more than 26 000 professional visitors, especially from emerging markets such as ASEAN countries and regions, and Africa.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IFSEC SA 2013</td>
<td>18 – 20 June 2013</td>
<td>Gallagher Convention Centre</td>
<td><a href="http://www.ifsecsa.com">www.ifsecsa.com</a></td>
</tr>
<tr>
<td>IFSEC SA 2013 is a chance for end users to meet their security providers face-to-face, while the channel can see what else is on offer in their areas of expertise. In other words, it is a smorgasbord of security options where visitors get to see the full spectrum of technologies and solutions applicable to their needs under one roof.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South African Institute of Security: Black Tie Bash</td>
<td>Saturday 17th August 2013</td>
<td>Injubulo Room, Indaba Hotel, Fourways</td>
<td>Tickets R500 per person or R4 750 per table of 10 Contact <a href="mailto:SAIS@tiscali.co.za">SAIS@tiscali.co.za</a> for more information.</td>
</tr>
<tr>
<td>CAMPROSA Conference</td>
<td>3 – 6 November 2013</td>
<td>Boardwalk Hotel and Conference Centre in Port Elizabeth</td>
<td><a href="http://www.camprosa.co.za">www.camprosa.co.za</a></td>
</tr>
</tbody>
</table>

Note: Any reader running public events related to the security industry are welcome to submit details of their events, training programmes or conferences for consideration. Items are published depending on space available and at the editor’s discretion.

---

### CCTV Surveillance Skills and Body Language Training Course

A two-day in-company course using extensive video incident material to show key learning points and focusing on:

- Observation skills
- The psychology of surveillance
- Body language and behavioural analysis
- Detection of incidents and recognition of risk indicators
- The evidence gathering process

This course is ideal for managers, supervisors, operators and investigators involved in CCTV surveillance or analysing video footage. Each course is trained personally by Dr Craig Donald

Tel: (011) 787 7811, e-mail: sales@leaderware.com, Web: www.leaderware.com
NOW IN ITS THIRD YEAR!

SECURE YOUR PLACE AT THE GREATEST SECURITY AND FIRE EVENT IN WEST AFRICA

- Nigeria has one of the highest economic growth rates in Africa
- Expand your business in an untapped and highly lucrative market
- Meet thousands of senior decision-makers and buyers from Government and Private Sector
- Supported by Government and major Industry Associations
- State-of-the-art exhibition venue

FOR MORE INFORMATION CONTACT US:

AFRICA
Baytir Samba
Project Manager
E: baytir.samba@ubm.com
T: +234 (0) 70 3742 2199
T: +44 (0) 20 7521 8007

INTERNATIONAL
Neema Patel
Sales Manager
E: neema.patel@ubm.com
T: +44 (0) 207 921 8614

SOUTH AFRICA
Jaques Swanepoel
Sales Executive
E: jaquess@montgomeryafrica.com
T: +27 (0) 11 835 1565

www.ifsecwestafrica.com
Security industry loses Terry Scallan

By Errol Peace, Chairman, South African Institute of Security.

It is with great sadness that we bid farewell to one of our pillars of reform in the private security industry. After a long illness Terry Scallan passed away in the early hours of Thursday 1 November 2012.

After being discharged from the permanent force of the military intelligence with the rank of Lieutenant Colonel, Terry has ever since been actively involved in the private security industry.

He joined the South African Institute of Security in 2000 and was elected to the Board of Governors in 2005. He was elected chairman of the board in 2008 and stepped down due to ill health in 2010.

During his term as chairman he was instrumental in forging the links with the UK Institute and the IISSM in India, where SAIS members enjoy reciprocal membership.

His involvement with SASSETA during the 2010 World Soccer tournament allowed Terry to play a very important role and was personally involved with the drafting of the Security at an Event unit standard. He was the SASSETA / SAIS liaison representative for the past six years and was elected to the SASSETA Chamber in 2011.

Terry was a renowned speaker on private security and training both nationally and internationally, and his training column appeared in the monthly security publications.

He was a tireless champion, an advocate and demonstrated immense passion about raising the skills set of security practitioners in South Africa.

His passing will leave an enormous vacuum in our industry.

Terry is survived by his wife Agatha and his sons, Gareth and Jared. We extend our condolences to them.

Register as an electric fence system installer

By Andrew Seldon.

We all know that anyone hiring an installer or integrator must ensure the service provider is registered with PSIRA. Sadly, while it’s illegal to hire someone or retain a company that is not registered to handle a security service or installation for you, the public is mostly unaware of this regulation.

New amendments to the Occupational Health and Safety Act that will come into effect in 2013 require all people and companies that work with electric fences to be registered (or licensed, if you will) with the Department of Labour. Not only does this change the nature of security work on electric fences, but should provide the public and businesses with a degree of confidence that registered companies can actually do the job properly and safely.

In order to be registered by the Chief Inspector as an Electric Fence System Installer as defined in the Electrical Machinery Regulations, 2012, promulgated by Government Notice R.242 of 25 March 2011, the applicant must submit his/her/its documents to the Chief Inspector to be considered for registration:

• Completed application form;
• Proof of experience on electric fence systems (letters from employers and letter of recommendation from the South African Electric Fence Installers Association or the South African Intruder Detection Services Association);
• Proof of working knowledge of the legislation and relevant health and safety standards applicable to electric fence systems (letter of recommendation from the South African Electric Fence Installers Association or the South African Intruder Detection Services Association);
• Copy of applicant’s South African identification document;
• Two photo’s (25 mm x 30 mm) colour or black & white;
• Receipt of R120-00 payable at any Labour Centre or bank.

If successful, this will provide the applicant with a temporary registration that will be valid till the 30th of September 2013. The Department of Labour has inspectors in all provinces that will be available to assist with the application or log onto www.labour.gov.za for the latest information and application forms.

Forms will be available from all electric fencing distributors and manufacturers. The following organisations may also be contacted:

Department of Labour: Tel. no.: +27 (0)12 309 4000/4378
South African Electric Fence Installers Association
e-mail address: info@saefia.com
Fax to e-mail: 086 527 0374
Fax number: 0866 499 588
www.saefia.co.za
South African Intruder Detection Services Association
e-mail address: saidsa@mweb.co.za
Tel number: +27 (0)11 845 4870
Fax number: +27 (0)11 845 4850
www.saidsa.co.za
Identity-based fraud is costing South Africa billions of rands. A leading local retail group is apparently suffering losses of up to R12 million a month. At one South African vehicle finance company, 60% of credit applications have documentation problems, with 30% of applicants supplying fraudulent identities.

The local healthcare industry also reports losses of as much as R13 billion a year, with a high proportion directly caused by identity fraud. In order to counter such astonishing losses, a new identity fraud prevention service called Identicate was launched late last year during a business breakfast at Fairlawns Hotel in Morningside, Johannesburg.

Xpert Decision Systems (XDS), the first and only 100% black owned credit information bureau, supported by Ideco Biometric Security Solutions created Identicate to actively combat identity fraud. Based on digital fingerprint verification, Identicate creates a link between demographic data (e.g. name, address, ID number) and fingerprint data to provide the fastest, most accurate way to authenticate consumer identity.

“Identicate allows sharing of fraud data. This is urgently needed to reinforce security and minimise risk across different companies. As a potent antidote to fraud, Identicate also highlights identity fraudsters and protects suppliers and consumers,” says Vivian Pather, MD of XDS.

“This seriously large scale use of the top fingerprint technology proves two things beyond doubt,” says Marius Coetzee, managing director of Ideco. “Firstly, the technology is tried, tested and proven. Secondly, it’s well-accepted by millions of local people who are accustomed to using it on a daily basis.

“The launch of Identicate means a stricter watch will be placed on consumer data and on information bureaux like XDS who process this information. Identicate makes it simpler and faster for us to ensure accuracy and safeguard data for consumers and the organisations who need this information. It will also protect South African business by ensuring that accurate identity-based information is rapidly available to avoid the increasing losses caused by a wide variety of identity frauds,” concludes Pather.

For more information contact Ideco Biometric Security Solutions, 086 104 3326, contact@ideco.co.za, www.ideco.co.za

US-based Arecont Vision has made a channel strategy change for its business in South Africa. Arecont has replaced a number of regional partners with two master distributors, Reditron (formerly Norbain South Africa) and Zela-Tech.

Arecont’s regional director, Ethan Maxon, says: “After a number of trips and discussions with trusted South African partners over the past few years, we realised two truths about this part of the world: (1) Like most places, the physical security market is a small community of professionals. (2) It is a region that believes in the distribution model. We moved our channel strategy to mirror these two truths by limiting our number of partners and ensuring those partners have extensive IP networking experience.

“Reditron and Zela-Tech have proven their commitment to continue driving the trend towards IP. It is this commitment and their experience in network design that were the primary reasons we chose to work through them as our master distributors. Going forward, there will be a local stock position of our more popular models that will dramatically improve turn-around times,” added Maxon.

For more information contact Arecont Vision, +1 951 440 0821, emaxon@arecontvision.com, www.arecontvision.com

Janine Ströh, a former production planner for a well-known manufacturer of electronic defence systems will be applying her considerable talents in her new role as production foreman for Centurion Systems.

Her current skill set will add value in this area, especially considering the complexity of the various electronic components being manufactured in this department. Janine has a sound knowledge of electronics, planning, scheduling and industrial engineering; skills which will allow her to make improvements to workflow processes and effectively manage people within this area.

The production foreman’s duties include the motivation and control of production staff, optimising electronic assembly production processes and recording and analysing production data.

She holds a Bachelor of Engineering degree from the University of Pretoria, and is currently studying towards her honours degree in Industrial Engineering.

For more information contact Centurion Systems, +27 (0)11 699 2467, adam.butchart@centurionsystems.co.za, www.centsys.co.za
**Hikvision and Avigilon team up**

Hikvision has announced that its ONVIF-conformant IP cameras now have the ability to seamlessly integrate with Avigilon’s Control Center Software. This integration now provides customers with the freedom to better choose the specific combination of products to best fit their needs.

Hikvision ONVIF-conformant IP camera models – bullet cameras, dome cameras, and box cameras – all boast advanced features, such as high resolution, wide dynamic range, low light capability, ease of installation, and many more. Moreover, its IP cameras provide users an open-standard based solution and great flexibility to select components for their security system.

With the Avigilon Control Center software, users can remotely monitor and control most of the key features of their Hikvision IP cameras; such as PTZ, two-way audio, alarm inputs, outputs, etc. Advantages of the software include multi-megapixel and high dynamic imaging, HD recording and playback timeline, data protection and storage management, to name but a few.

“Hikvision IP cameras already provide clear video, while the Avigilon Control Center is engineered to manage HD videos, and efficiently handle bandwidth and storage,” says Keen Yao, international marketing director of Hikvision. “Additionally, this cooperation with Avigilon will truly benefit our mutual customer base and helps them achieve a more flexible and scalable IP-based surveillance system.”

“We believe openness benefits our customers and partners, and this integration will provide them access to the most appropriate solutions,” says Keith Maret, vice president of marketing and communications at Avigilon. “By ensuring our products are ONVIF-compliant, we are helping bring the industry closer to standardisation.”

For more information contact Hikvision, +86 571 8700 6060, wulin@hikvision.com, www.hikvision.com

**Safer cash handling for retailers**

G4S Cash Solutions South Africa is offering tenants at The Gateway Theatre of Shopping peace of mind through a convenient, efficient and secure online cash collection and processing solution.

The way it works is the tenant simply secures the cash in a tamper-evident security bag for collection and captures details of the cash deposit on a secure G4S Web portal. An unarmed security officer will arrive to collect the cash and take it to the on-site cash processing centre.

The cash is then transported using a secure cross-pavement carrier (CPC). Should a criminal remove the cash from the security officer, the CPC’s dye stain technology will activate and render the bank notes unusable. At the cash processing centre, the deposit will be verified under watch of CCTV against the data the tenant captured on the Web. Tenants that don’t have Internet access can also make use of the cash processing service, with G4S capturing the deposit data on their behalf.

Says Albert Erasmus, MD of G4S Cash Solutions: “No longer do Gateway tenants need to arrange for armed cash collection or ask their staff to take their cash to the bank to be deposited. This solution increases safety for tenants, shoppers and in-store workers at Gateway stores by offering a gun-free cash collection service.”

Erasmus continues: “In addition to the security benefits, our cash collection and processing services spares stores and their employees the time they used to waste queuing in the bank to deposit cash. Staff can focus on their jobs rather than banking. It also makes it easier for store owners to track and reconcile cash deposits, thanks to the electronic audit trail the solution offers.”

Store owners will know how much money is to be banked and when it is deposited – especially helpful for those monitoring cash across a number of stores remotely. A fully automated discrepancy management process notifies customers via e-mail as soon as a discrepancy is noted at the cash processing centre.

**UTC Fire & Security’s Integrated Security Experience**

UTC Fire & Security recently held a customer event under the banner of the Integrated Security Experience. The presentations focused on the various product offerings for the security market from UTC, but with a focus on integration.

Brent Cary, regional manager sub-Saharan Africa, for UTC’s Lenel brand, presented on the various successes UTC’s brands have been part of over the years. These include being the company that created the space suit worn by the late Neil Armstrong for the first moon landing, through to the company responsible for the largest single private networked CCTV system in the world, the Paris metro and bus system which includes 12 000 cameras in the trains and 25 000 cameras in the busses.

UTC’s TruVision platform is also responsible for one of the largest video installations in South Africa at SA Diamond.

Cary noted that success in large projects is not simply a matter of selecting the right product, but due to the effective integration of various systems. “The key talking point at the event was the difference between interfacing, which any company can do and integration, which UTC does seamlessly with all of our products and a host of third-party products.”

An interface is where two or more separate software products communicate under limited capacity. Data is maintained in multiple locations; thus, requiring more administration. A fully integrated system means that the products are one. This happens when two or more products work closely together to combine different functionalities into one product. In real integration, the data is maintained in one location.

“System integration is about adding value to the system,” explained Cary, “and the resulting capabilities that are possible because of seamless interaction between the subsystems.”

The four brands discussed at the event where:

- **TruPortal:** UTC’s entry-level, licence-free, access control platform with simple control and monitoring from a Web browser or iPad application. The TruPortal system integrates with the TruVision TVR10 range of video products.
- **IFS:** UTC’s fibre and networking range of products that offer cost-effective solutions to convert your video to fibre.
- **TruVision and UltraView:** TruVision and UltraView are UTC’s CCTV/video ranges that consist of analogue, IP and hybrid solutions for all surveillance requirements. Both these product ranges seamlessly integrate into UTC’s Alliance, as well as the Facility Commander Wnx security management platforms.
- **Lenel:** Lenel is UTC’s high-end enterprise solution that allows customers to seamlessly integrate all aspects of their security, not only from UTC’s access control, fire detection, CCTV and intrusion product range, but also from a large number of third-party companies through its OAAP programme.

For more information contact UTC Fire & Security, +27 (0)11 579 7300, gretchen.geldenhuys@fs.utc.com, www.utcfireandsecurity.com
Trust the name that leads the Industry

Coaxial network/CCTV protection

Coaxial protection for high speed data transmission lines. Suitable for CCTV applications. These devices exhibit negligible insertion loss and are fitted in line at the equipment connection.

CCTV Signal and PSU Protector

Coaxial protection for high speed data transmission lines. Suitable for CCTV applications. They protect both the CCTV signal as well as the DC power supply voltage. These devices exhibit negligible insertion loss and are fitted in line at the equipment connection.

CCTV Fibre Optic Interface

The optic video link consists of a receiver and transmitter unit. Both units and fibre cables are immune to EMI/RFI, eliminating any need for concern in noisy environments. Clearline fibre optic transceivers are easy to install and isolate your CCTV systems from lightning damage.

CCTV 16 way Protection Rack

This Rack has 16 units for coaxial protection for high speed data transmission lines. Suitable for CCTV Systems. These devices exhibit negligible insertion loss and are fitted in-line at the equipment connection.
SASA responds to the Minister

In Parliament recently, the Minister of Police, the Honourable Nathi Mthethwa, touched on a range of issues around the private security industry of South Africa. SASA has listened and has taken heed of the Minister's pronouncements, some of which were helpful and enlightening while others merit a word or two from the Association.

Minister Nathi Mthethwa: The amendment bill is aimed at eradicating criminality in the private security industry.

Jenny Reid: The problem is not the general private security industry. One of the bigger problems is the non-compliance in the security industry which PSIRA does not appear to be able to control. Putting more regulations in place and not policing them is pointless.

The Minister: The Bill seeks to address identified security threats, risk and problems regarding the regulation of the private security industry.

Reid: I believe that this is necessary but it needs to be done in conjunction with the private security industry. It is easy to meet with the larger compliant organisations which have regulated addresses and comfortable offices serving tea and coffee. What is being done about the small organisations that do not employ legally and do not operate legally?

The Minister: The South African private security industry is increasingly performing functions which used to be the sole preserve of the police. This has, and will continue to have a serious influence on the functioning of the criminal justice system as a whole. While it is true that private security does and can fill certain vacancies, private security can never replace the public police.

Reid: I agree 100% with this and it is all the more reason why we should be working more closely together as opposed to pulling apart. The police often do not have the skills or resources that are available to the private security industry. Would it not make sense for both parties to serve the people? We would certainly welcome such a partnership.

The Minister: The police aim to protect the public while private security has a profit motive and has as its main objective the protection of its client’s interests. The interests of private clients and those of the state and public are not always the same.

Reid: Private companies are in business to make a profit and the security sector is no exception. And what they add to the economy while doing so cannot be ignored. Our security companies operate in what is probably the world’s most competitive industry. We employ over a million people. We contribute billions of rands to the tax base while doing our part to deliver as safe an environment as possible. If the industry did not function as efficiently as it does, the country would be in turmoil.

The Minister: Part of this amendment is aimed at eradicating the criminality within this industry. Clearly, the ability of criminal networks to infiltrate the industry and the vulnerability of the industry to such infiltration poses a major threat to the government’s capacity to address crime.

We listened, we understood, but we’d just like to add . . .

Reid: Why would criminal networks only want to infiltrate the security industry? We need to deal with crime as a whole – South Africa rates very highly on the scale of crime. I do not believe any research shows that the security industry has a high level of syndicate infiltration. Do the police have the resources to deal with the syndicate crime infesting such high profile areas as banking, cash in transport facilities, the information technology, industry and the retail sector?

The Minister: An indication of the extent of criminal infiltration of the industry can be seen in the results of a voluntary vetting process initiated by some private security business in 2008 where 170 728 guards were vetted through the SAPS Criminal Records Centre, 14 729 were flagged as being linked to possible criminal activities. All these guards allegedly had valid registration certificates as required under the Private Security Industry Regulatory Act, 2001.

Reid: This is a massive problem because PSIRA only request that a security officer is screened on registration in the industry. The bigger more compliant companies do regular screening. I do not believe the fly-by-nights or non-compliant companies do any form of screening. Again it needs to be an effort between the industry and PSIRA.

The Minister: The ICoC essentially promotes international self-regulation of the industry and while the move may be welcomed, some commentators have expressed concern that this initiative cannot replace, and should not circumvent, moves to implement effective international instruments through the United Nations.

Reid: SASA is currently trying to drive compliance but we are not the regulatory body and the current regulatory body often does not follow up on reports of non-compliance. We have had a process in place to strengthen this area which must be driven by PSIRA, and we have repeatedly emphasised that we are ready and willing to participate and assist.

The Bill also seeks to limit foreign ownership in private security companies to 49% and gives the minister the power to determine the percentage of foreign ownership and control.

Let me quote the DA member of parliament, Diane Kohler-Barnard, on this point: “This is nothing short of expropriation – and should 51% of the shares in the company be sold to a South African, there is no guarantee that the shares will not then be sold on to a foreigner. It also claims that permanent residents (foreigners granted the right to live and work here) may not be involved in this industry. This is clearly illegal.”

Finally, we have always stated that the private security industry exists in South Africa because there is a need for it. We fulfil a role that the police cannot – simply because of the numbers needed to address the tide of crime, because state budgets do not and cannot fund the real security requirement and because the security requirement will continue to increase for the foreseeable future.

It makes no sense to eviscerate the private security industry. It’s a fact that private security personnel registered in accordance with PSIRA rules outnumber SAPS employees by four to one. This statistic is not lost on SAPS, evidenced by the fact that the minister has a bill before parliament that seeks to change existing laws that govern the industry.

To the government we would say: “We can help, we really can. Don’t keep us at arm’s length. Let’s work as a team. South Africa will be the winner.”
Now in its third year, IFSEC West Africa 2013, sponsored by Guardia Systems, will take place at the EKO EXPO Centre in Lagos from 5-6 March 2013.

As a respected commercial and government security, fire and safety event, it has become an increasingly attractive destination for those security professionals looking to source innovative products and strategic solutions for all their security needs.

"With tight budgets and changing legislation, security professionals must often make strategic purchasing decisions that will impact on their organisations," believes Ross Cullingworth, portfolio director at UBM Montgomery West Africa, the organisers of IFSEC West Africa 2013. "This show is ideal for these professionals as it opens up an abundant marketplace for them to compare products from top local and international suppliers, manufacturers and distributors, some of which have never been seen before – so this will be a first look at what buyers can expect in the future."

Every year, more visitors flock to IFSEC West Africa and the 2013 event is expected to draw over 2,000 security and safety professionals to Lagos, many of which will be welcomed as first-time visitors.

“We believe the market is recognising the intrinsic value of the show, as it educates visitors in an interactive environment and empowers them to make the right decisions right there and then,” he comments.

“At the show, visitors can compare products and supplier offerings. We’re confident that they will discover a product or service to meet any security challenge. There is no need to spend months searching for solutions, especially in today’s driven and time-scarce environment."

Besides showcasing top security brands, IFSEC West Africa 2013 will once again be a hub of education, keeping visitors abreast of the latest industry trends. From product launches to seminars, it will enable visitors to keep up to date on important issues. There will be a panel of high-profile industry experts to speak about implementation, as well as share best practice examples and useful case studies.

West Africa has established itself as an international destination with a uniquely African character; as such, IFSEC West Africa attracts exhibitors and visitors from all over the world. “It’s an ideal place for extending your network of contacts,” Cullingworth says. “For us, it’s always exciting to be a part of such a synergistic event – with people meeting, debating and exchanging ideas that will shape the security landscape for the next few years.”

IFSEC West Africa 2013 includes a new Safety Pavilion, a dedicated exhibition area, where visitors can witness the most innovative safety solutions up close for vivid and educational demonstrations throughout the two-day event.

To find out more about exhibiting or visiting at IFSEC West Africa, visit www.ifsecwestafrica.com
Errol Peace, MD of BTC Training and Chairman of SAIS, is concerned about the lack of progress in the promulgation of the skills programmes for the security industry.

“The outdated Grades A to E need to be urgently replaced by the proposed Skills Levels 1 to 5, which are geared around increasing the industry-relevant skills of the learners. The old system merely provided training, without imparting any skills transfer,” said Peace.

Companies offering skills programme learnerships to their employees are currently entitled to a discretionary grant. “What is interesting is that the security industry currently pays the largest portion of SASSETA funds and yet, ironically, we receive the smallest return on discretionary grants. We have 400 000 registered security officers, but only 50 discretionary grants have been awarded for the year. This simply does not make sense,” Peace continued.

In recent media comment by Minister of Police, Nathi Mthethwa, much emphasis is placed on the threats, risks and problems regarding the regulation of the private security industry. Minister Mthethwa said that: “…the ability of criminal networks to infiltrate the industry and the vulnerability of the industry to such infiltration poses a major threat to the government’s capacity to address crime.”

Minister Mthethwa further discussed the promulgation of the Private Security Industry Regulation Amendment Bill, which seeks to limit foreign ownership in private security companies to 49%.

“My contention is that no mention is made of the progress of acceptance and authorisation of the much-needed skills programmes. The previous reasons given for not rubber-stamping the programmes were the volume of content and the cost of learnerships. By reducing the content, we have also concurrently been able to reduce the cost of learnerships. Given this, there should be absolutely no reason for the programmes now not being promulgated,” Peace concluded.

For more information, contact Errol Peace at epeace@netactive.co.za

| IFSEC South Africa 2013 |

After almost two decades, IFSEC South Africa remains the largest security and fire exhibition of its kind in Africa. Organisers UBM Montgomery are now preparing for IFSEC South Africa 2013, from 18-20 June 2013, at Gallagher Convention Centre in Midrand.

Designed around the needs of security professionals and offering a platform for exhibitors to showcase their latest technologies, IFSEC South Africa is now established as an important event for stakeholders across all disciplines within the security sector.

Ross Cullingworth, portfolio director at UBM Montgomery says the next show will build on this success. “We had almost 6 000 visitors at last year’s show from government, trade and end-user markets;” he reports.

IFSEC South Africa is a premier platform for leading companies to highlight the latest security and fire technology and services to key decision-makers and buyers. Top visitor profiles come from a wide-range of industries, including: installers, suppliers/distributors, security consultants, system integrators, IT/networking/telecoms representatives and manufacturers.

IFSEC South Africa 2013 will be upgraded to offer even more experiential features, educational seminars and networking opportunities, as well as the innovative exhibits visitors in the fire and safety sector have come to expect from the information-packed and interactive three-day event.

IFSEC South Africa 2013 will include the launch of a dedicated fire pavilion, providing those exhibitors that specialise in fire safety products and solutions with the ideal opportunity to showcase products and services alongside a seminar programme. The IFSEC South Africa 2013 fire pavilion will provide an opportunity for visitors to see and compare the widest range of fire solutions while networking with industry experts from all aspects of fire safety.

Global investment in security-related industries is growing; it is estimated to be worth about $60 billion, according to trend watchers at PricewaterhouseCoopers in a report late last year. “Since 1998, when the economy took a tumble, security companies are fighting to keep their market share,” says Cullingworth. “We believe security brands want to maintain or improve their image with consumers amid news stories that continually show the perils to public and government security. Terrorism activity,” he further points out, “always remains a threat no one can ignore.”


“It’s a great opportunity for exhibitors to touch base with government representatives that hope to build national resilience, counter-terrorism, border security, national surveillance and stronger police forces,” Cullingworth explains. “We’ve also lined up some of the best thought leaders and industry strategists for a lively conference at the exhibition.”

Furthermore, IFSEC South Africa 2013 incorporates OSH EXPO Africa 2013, an event which is fast becoming the destination for exhibitors to launch and showcase the latest occupational safety and health products. Having launched for the first time in 2011, the show is already gaining tremendous momentum in the industry. OSH EXPO Africa 2012 welcomed 2 661 visitors, a 21% increase on the previous year.

To find out more about exhibiting at IFSEC South Africa contact Charlene Hefer, UBM Montgomery on +27 (0)11 835 1565, charleneh@specialised.com, www.ifsecsa.com.

What’s happening with skills training?

By Allyson Koekhoven.

Errol Peace, MD of BTC Training and Chairman of SAIS, is concerned about the lack of progress in the promulgation of the skills programmes for the security industry.

“The outdated Grades A to E need to be urgently replaced by the proposed Skills Levels 1 to 5, which are geared around increasing the industry-relevant skills of the learners. The old system merely provided training, without imparting any skills transfer,” said Peace.

Companies offering skills programme learnerships to their employees are currently entitled to a discretionary grant. “What is interesting is that the security industry currently pays the largest portion of SASSETA funds and yet, ironically, we receive the smallest return on discretionary grants. We have 400 000 registered security officers, but only 50 discretionary grants have been awarded for the year. This simply does not make sense;” Peace continued.

In recent media comment by Minister of Police, Nathi Mthethwa, much emphasis is placed on the threats, risks and problems regarding the regulation of the private security industry. Minister Mthethwa said that: “…the ability of criminal networks to infiltrate the industry and the vulnerability of the industry to such infiltration poses a major threat to the government’s capacity to address crime.”

Minister Mthethwa further discussed the promulgation of the Private Security Industry Regulation Amendment Bill, which seeks to limit foreign ownership in private security companies to 49%.

“My contention is that no mention is made of the progress of acceptance and authorisation of the much-needed skills programmes. The previous reasons given for not rubber-stamping the programmes were the volume of content and the cost of learnerships. By reducing the content, we have also concurrently been able to reduce the cost of learnerships. Given this, there should be absolutely no reason for the programmes now not being promulgated,” Peace concluded.

For more information, contact Errol Peace at epeace@netactive.co.za
Camsecure restructuring broadens scope

Over a two-year period Camsecure has tripled in size and turnover, prompting the company to restructure its operations. This projects-based security solutions company was formed almost ten years ago and provides open platform technological solutions to its client base throughout Africa using off-the-shelf IP equipment.

“We have reached and even surpassed all the goals we put in place when we started out as a small, three-person organisation,” says MD, Francois Malan. “As the demand for our IP surveillance services has grown, we have continually hit new milestones over the last ten years. In order to continue our growth and achieve high service levels, we identified key focus areas within the company that we have streamlined. We have also implemented some ground-breaking procedures that have improved our operational efficiency.

“We have identified the key areas in our business and given trustworthy people the responsibility to manage these areas. We have put in strict systems and software to monitor and audit all levels of our business and we feel extremely confident that Camsecure is more than adequately geared for any work that may come our way.

“We have a very strong board of directors in place, headed by our chairman, Sipho Mseleku, formerly chairman of the SADC Business Chamber. Camsecure has also achieved a high BEE rating. Under the new structure we have Danie Malan, formerly deputy president of the National Olympic Committee, as CEO; Francois Malan as MD and William Muller as Gm,” Malan says.

“The rest of our organisation currently resides under three pillars, administration, operations and sales. The main additions to our administration department are a financial manager, Anita Peters; human resources manager, Alice Mothiba; and legal compliance and safety manager, Gerhard Vorster,” notes Malan.

Operations manager, Theuns Brits, heads the operations division and a number of senior technicians of various grades report to the projects manager, Christo Deyse. The sales regions operate under Western Cape regional manager, Vivian de Meillon and Northwest Business development manager, Frans Deysel. The rest of South Africa and the African region operate from Camsecure’s Johannesburg head office.

The company concentrated on its project management and customer relationship offering and determined that it needed to address its policies and procedures from a legal and organisational perspective. “This was followed by an overview of our operational procedures to ensure that we have all the checks and balances in place to continue providing a superior product and service offering. This forms part of our vision to deliver high-end project management packages to our client base,” Malan says.

Camsecure supplies only those products that it believes adhere to the stringent quality measures the company adopts. “We have aligned ourselves with international suppliers of best practice hardware and software, such as Axis network cameras, Milestone video management software, DDN storage solutions and Adani X-Ray Scanners. By being selective about our product offering, we are able to ensure repeatability in positive outcomes,” Malan says.

For more information contact Camsecure, +27 (0)11 781 1341, francois@camsecure.co.za, www.camsecure.co.za
The behaviour of cars

By Dr Craig Donald.

Vehicles play a prominent role in creating opportunities, assisting and providing an escape method when an incident is committed. Although cars themselves have no intrinsic behaviour, the people who use them create variations in movement and use that can directly indicate that an incident is in the process of occurring or will occur. A car with random movement patterns, driving slowly, tinted windows, number plate issues and occupied by three or more personnel create an awareness among any surveillance person that something suspicious is occurring. By being sensitive to these signs, operators have a good chance of spotting and responding to incident conditions.

Some time ago I was having some discussions with an associate in the UK who was discussing how intelligence could be used to assist in crime detection. While we use, or should use intelligence extensively in South Africa to assist us in target identification and crime pattern analysis and interrogation, he gave an example with the police that was slightly different in perspective. He discussed how police had used a number plate recognition system to identify vehicles which were not up to date on their registration, or where the number plates were inconsistent with the vehicles involved.

Police a few kilometres up the road would then pull the vehicles over for a stop and search, speak to the drivers and check the vehicles. It was found in a sizable percentage, illegal or stolen goods were found in the vehicles or that the drivers themselves were wanted in connection with some crime incident. The important point here is that psychological behaviour associated with law breaking while driving without a valid registration was associated with law breaking in other areas.

The importance of procedures

The violation of procedures or law in one area has a great deal of relevance. If we have a look at mining sites for example, breaking of safety procedures by not wearing safety equipment is often associated with theft of precious minerals – for example, not wearing safety gloves allows a criminal to more easily access and remove gold or diamonds. Similarly, casinos institute procedures at gaming tables to control the actions and reduce the chance of personnel or guests doing something that could actively lead to cheats, scams or theft. It is not just these industries, however. Procedures are an essential way of controlling and reducing the potential for theft in many other industries as well. In addition to this, they cost very little although they may introduce some slowdown or process due to checking. Of major concern at times is that management don’t understand or appreciate the importance of procedures and the cost of violations.

It is quite understandable, therefore, that behaviours of cars in terms of road traffic transgressions could identify a consistent trend of other illegal activities. Those who bear no regard for road rules are likely to have little concern for other legal requirements. It seems that traffic departments are missing out on an important part of this principle. While roadblocks do contribute to identifying people with unpaid speeding fines and at times more serious offences, they are more or less random in nature.

Equally, although I was taught that when setting up a roadblock, one should always have representatives hidden well before the roadblock to detect vehicles turning around when they see the road block, I have seen a number of such vehicles turn around without any consequence before arriving at the stopping point in South Africa. These kinds of actions identify immediate suspects and just stopping them alone may have made the process worthwhile, yet such behaviour is not anticipated and acted on in the majority of cases I have seen.

Effective policing

However, a more important concept is that if police resources were used to identify transgressions or moving violations on the road, they would likely find far more criminals and have far more success in catching wanted people than random stopping at roadblocks. I can’t feel that somehow they are missing an important area in both crime prevention (apprehension of offenders of moving violations sends a message to other road users) as well as suspect detection. The use of number plate recognition or toll plaza records show a whole potential side to identifying vehicles associated with being in an area where crimes have been committed around certain times.

Whether police act on car behaviour or not, there is a range of indicators that show surveillance operators that something is wrong. Placement of cars near an entrance of a bank or a casino, particularly if this is on the kerb or in a no parking area show potential for an armed robbery. Cars stopped for prolonged times with no people getting in an out shows possible intent, or people approach such a vehicle for a short time and moving away shows potential deals associated with drug dealing.

Car thieves will often park their vehicle next to the one being stolen, and where this occurs with lots of available parking in other areas it should raise immediate questions. Things like thermal signatures on cars indicating recent movement can also assist in detection and investigations. People’s behaviour therefore makes for an interesting perspective on the criminally inclined behaviour of cars.

Dr Craig Donald is a human factors specialist in security and CCTV. He is a director of Leaderware which provides instruments for the selection of CCTV operators, X-ray screeners and other security personnel in major operations around the world. He also runs CCTV Surveillance Skills and Body Language, and Advanced Surveillance Body Language courses for CCTV operators, supervisors and managers internationally, and consults on CCTV management. He can be contacted on +27 (0)11 787 7811 or craig.donald@leaderware.com
Comb Communications (Pty) Ltd

Mobile Internet

GSM Intercom
- Sim chip on board
- RX
- TAP TAP (2)

Programmable anywhere, anytime

Nova Loader
- First in the world
- Manage remotes via the web

Nova Remotes (5000)

Ideal for townhouses, complexes, estates and business parks

System Features
- 4 Relays and 6 Inputs
- On-board receiver
- 3 Phone numbers per unit
- Pin codes
- Time barring
- Guard call
- Free exit control
- SMS alerts
- 3 Keypads
- Call line identification
- Missed call gate opening

Web Features
- Remote programmability
- Reliable reporting
- Bulk SMS
- Bulk e-mails
- Manage remotes
- Manage residents entry
- Manage telephone no’s and pins

Related Products
- TAP TAP
- Tap Ex
- Nova Loader
- Nova Remotes

Tel: 011 089 5800
Web: www.comb-communications.com
Email: sales@comb-communications.com
A type of paranoia is stealthily finding its way into the workplaces of the world’s developed nations. It might be an echo of George Orwell’s 1984 in a rebirth of Big Brother, this time in human and/or digital form. This kind of creepiness is increasingly worrying US workers under workplace surveillance.

Answers investigators are trying to find centre on whether or not intelligence gathering in the workplace, overtly or covertly, is ethical or legal. Some of the more cynical maintain that if workers are innocent of anything underhand, they won’t mind being spied upon, and might even enjoy displaying their morality. More liberal indignation insists that privacy is a human and civic right and that no one or no thing is permitted to invade it.

That point of view, however, is not universally held, and even exists in different layers depending where in the world you happen to be. The law and the ethicists regard the issue differently in Japan, for example, to the way it is held in the United States.

To confound matters even further, the definition of privacy differs widely wherever you go. In South Africa, for example, you won’t be committing a crime if you spy on someone, but you could find yourself on the wrong side of an expensive civil suit.

Some sort of universality occurs in the separation of surveillance of employees in the workplace and outside of it. The majority of such laws state implicitly that employers must limit their intelligence gathering to areas related to work. For example, tracing employee’s company telephones, cell phones and accessing e-mail accounts are permissible, but tapping home phones or hacking into their private e-mail systems are not. Employers, in most jurisdictions, are not required to inform their staff that they are being surreptitiously monitored. An argument for the ‘yes’ brigade is that staff members will be less inclined to dishonesty if they knew they were on camera. The opposing view maintains that overt surveillance simply drives the bad element underground and makes them more difficult to identify and to get the goods on.

Productivity versus conflict
If companies decide to be up-front with their surveillance policy, they might immediately face a divided staff with some in favour and others against, leading to long wrangling, arguments, delays and unhappiness.

The employer’s job is to minimise the number of dissatisfied workers by convincing them that monitoring is ultimately beneficial.

And what of those companies who do not have workplace surveillance, and want to install it? It’s a given that some workers will protest strongly. For that matter, does an employer tell new staff members before they are hired that they will be monitored after they’ve been taken on or not at all?

How this scenario is unfolding is of as much interest to labour unions as it is to management. Bosses are finding that a well established, wide-coverage picture and sound system of workforce activity can often yield valuable information on labour union matters.

Shop stewards worry that such loosely gathered intelligence can forewarn managers of impending union activity and even forestall shop floor action. And labour spies can be recruited by either labour unions or employers with a similar goal – to find out what the other is thinking or doing.

Legal espionage?
According to Wikipedia, a labour spy is someone recruited or employed to gather intelligence, commit sabotage, sow dissent or engage in other such activities, typically within a corporate entity.

Does it get that far in South Africa? Undoubtedly, and there are many case histories to prove it.

Labour spying and industrial espionage are discreet bedfellows and there is little to differentiate their behaviour in reaping the information or result they require. Each uses stealth to gather intellectual and sensitive data often in an unethical manner with the aim of getting the edge on the other side.

In South Africa, labour spying or industrial espionage per se is not unlawful, but perpetrators could be nabbed under other such illegal activities as theft or trespassing. The underlying philosophy of industrial espionage is, why spend years and millions of Rands on research and development constructing a customer base when you can bribe an employee in the competitor’s camp for a few rand, tap their telephones or bug their offices.

This is a complex and fascinating subject and it concerns us all. I’ll resume the journey in future editorials.

For more information contact iFacts, +27 (0)82 600 8225, jenny@ifacts.co.za

OPINION

Someone’s watching me
By Jenny Reid.

Just what does invasion of privacy really mean?

By Jenny Reid.
UPS Xcellence

3KVA M-Series UPS
- LCD display
- Internal batteries
- Rack mountable/tower
- Wide input voltage
- Online double conversion
- Pure sine wave

SNMP Network Adaptor
- Input/output voltage
- Control UPS from network
- Remote self-tests
- Load/temperature/battery display

Battery Pack
- Matching design
- Internal charger
- LED display
- Up to 4 battery banks per UPS
- Battery test function

Johannesburg
+27 (0)11 608 4259
sales@pss.co.za

Cape Town
+27 (0)21 552 2339
capesales@pss.co.za

Durban
+27 (0)31 303 3902
kznsales@pss.co.za

Pretoria
+27 (0)12 342 0436
plasales@pss.co.za

www.pss.co.za

Inverter  UPS  Solar Panels  Batteries
A real security solution

By Andre Mundell, director at Alwinco.

Security providers and suppliers are not equipped to do security risk assessments.

I want to tell you a story about why an independent security risk assessment is different from a risk assessment done by a security provider.

A few years back we a new client phoned us with a recurring problem. Criminals had captured one of the guards on the premises and used his radio to establish the whereabouts of the rest of the security team. After capturing the entire security staff, they had been able to rob the company of assets worth thousands.

The client had switched security providers only to have this scenario repeated another four times. Each of these security providers had ostensibly performed a security risk assessment on the property, but they had all recommended solutions which matched the services and products that they offered rather than tailoring solutions to their client’s needs.

We were then asked to do a security risk assessment on the premises in question.

After identifying all the relevant issues the client finally understood how and where the criminals were gaining access to the property and came to the following conclusions:

• The previous security companies had not considered effective lighting options.
• They had not considered thermal products while the neighbourhood and premises itself were very dark, and some of these security providers did not even know the basics of how thermal products work.

Because of the size and layout of the premises, we suggested the following:

• That their security service provider (Company A) be retained and allowed inside the premises.
• Because of the fact that criminals always managed to overpower and take these guards captive, we recommended that another security service provider (Company B), be placed on the outside of the premises in plain clothes.

After a few months, the same criminals attacked the client’s premises again. Company A had not been made aware of Company B, and there was no radio link between the two. This meant that the criminals also had no knowledge of Company B. Company B saw the guards from Company A being overpowered, reacted accordingly by informing the SAPS and their own armed reaction vehicles and in the end, the criminals were apprehended.

The above is a classic example of why security service providers cannot do security risk assessments, and also why they cannot tell you when they find risks that cannot be handled by one of their services or products. Hence the fact that it is imperative that companies employ the services of independent security risk assessors who will suggest real solutions to eliminate the client’s security risks as identified and explained in the final assessment. This in turn will allow the client to ensure that those risks are properly addressed as per the solutions suggested in the security plan.

No security company will advise a client to hire their competition to protect one area while they themselves protect another. Being independent and unaffiliated we were able to see the real risks involved and made solution based suggestions based on the client’s individual and working environment security needs.

It is better that a security risk assessment is done by an independent security risk assessor. Assessors cannot do an objective security risk assessment or ensure relevant and correct solutions if they are affiliated to any security provider or supplier.

Companies requesting security usually assume that their appointed security provider has done a security risk assessment; and most security providers will say that they have done a risk assessment. However, they will have performed a product assessment, not a security risk assessment. Security providers cannot and in most cases will not reveal your true risks to you.

I would like to stress to all corporate MDs, CEOs and small business owners the importance of protecting your company’s assets and employees. Gather all your facts before accepting any proposal for security services or products.

I again want to emphasise the fact that security providers and suppliers are not equipped to do security risk assessments. The fact that they are mandated to perform any and all assessments to reflect their service or product as the best option for you restricts them from being able to do effective and objective security risk assessments.

For more information contact Alwinco, +27 (0)71 319 4735, aviljoen@alwinco.co.za, www.alwinco.co.za
We understand that you want industry facts, updates and news whenever, wherever. Hi-Tech Security Solutions – the definitive information source for security, operations and risk management professionals – brings news and information to you in formats that best suit your lifestyle.

Monthly print and digital issues of Hi-Tech Security Solutions
Informed editorial content, trends and other industry news

CCTV Handbook + Access and Identity Management Handbook
In-depth and objective best practice guides

Electronic news briefs
Sent twice a week to update you on the latest news and technology

www.securitysa.com
Our on-line magazine that lets you find relevant content dating back 12 years!
Also available in mobile format

Hi-Tech Security Business Directory – Print/On-line
The security industry’s ultimate reference guide

Tel: +27 (0)11 543 5800
Circulation: subs@technews.co.za
Sales: vivienne@technews.co.za
www.technews.co.za

hi-tech security solutions
Your viewpoint from all angles

Your trusted technology news and information source
Successful security contracts

By Wayne Hermanson and Garth Briggs of Physical Risk.

Ensuring security consultants and service providers deliver what the customer wants.

Wayne Hermanson and Garth Briggs of Physical Risk offer advice on what contract a buyer should create to ensure his security consultants and service providers deliver what he wants instead of what they want. The first question we deal with is how customers should contract with a security management consultant to ensure they are suitably protected and will receive the services agreed to.

Hermanson says the manner in which customers contract the services of a security management consultant is key to the success of the professional relationship and should have a clear audit trail. The key outputs should form part of the contracting process as a minimum.

The initial client meeting is used to explore the customer’s service needs and devise a service proposal, should the customer does not already have the scope of services defined.

The service proposal is the source document for the description of the security management consulting services to be rendered by the SMC. Service proposals vary in format style, however there are a number of proposal elements that should be included to demonstrate the SMC’s expertise to perform the proposed services. These include but are not limited to the following:

- **Cover letter.** To thank the prospective customer for the opportunity to bid and highlight particular aspects of the proposal that should be examined closely.
- **What services will be rendered?** Be it assessment, design, project management or security management services.
- **How services will be rendered?** Methodology and measureable deliverables.
- **Who specifically will perform the services?** The engagement team of consultants should be named with their qualifications and experience listed.
- **Where/when will the services be rendered and what will the duration be?**
- **Company profile/background.** The consulting company’s historic background, philosophy, ethics, vendor/product neutrality and approach to the services requested should be explained.
- **Engagement considerations.** Items that may be included under this section include SMC and customer’s responsibilities, service/project timeline, limitations, exclusions, changes in project scope, fees, expenses and confidentiality.

Measuring ROI

In many cases customers know better what it requires from an independent SMC or consulting firm. It is certainly prudent to explore the customer’s service needs thoroughly during the initial and further client meetings. Once the SMC’s code of ethics with respect to a fixed fee structure for a fixed term has been dealt with, both parties may focus on understanding and defining service requirements to the customer’s satisfaction.

**Confidentiality agreement.** The SMC is likely to be privy to sensitive proprietary information and would have detail of the customer’s security vulnerabilities, which makes it important to have a confidentiality agreement signed.

**Service agreement.** The SMC’s agreement should be a performance agreement directly linked to the services to be performed, deliverables with cost and time constraints clearly defined.

**Project charter.** The project charter also referred to as the “Terms of Reference” document is drawn up once the customer has approved the service proposal and both parties have signed the confidentiality and service agreements. It constitutes the benchmark against which the SMC should be measured with respect to service delivery. The customer representative managing the SMC’s service delivery should approve the project charter and it serves as primary terms of reference at all progress meetings. Items to be included in the project charter include but are not limited to the following:

- **Service/project description.** This section should include a full description of the services required with relevant background and clear references in the case of tenders.
- **Service/project objectives.** This describes the essence of the SMC’s service deliveries expressed as customer outcome requirements.
- **Constraints.** It may include time and/or budget constraints or any other constraints imposed by the customer.
- **Assumptions.** The SMC shall define assumptions such as information that needs to be provided by the customer, assumed expenses, delays caused by the customer, payment of other service providers associated with the service/project, etc.
- **Reporting structure.** Who will the SMC report to for service deliverables and who shall approve payment of service invoices?
- **Deliverables.** A comprehensive list of each service deliverable in measureable terms.
- **Service activity time chart.** To indicate when the various deliverables shall be performed within the agreed timeline.
- **Fees and expenses.**
- **Acknowledgement of SMC commitment to project charter.**
- **Customer approval.**

Measuring performance is critical.

Performance should be measured against a comprehensive project charter that clearly defines the service objectives and outcomes.

At Physical Risk, we align performance measurement not only with the service requirements but also with the customer’s security risk profile. Our service delivery only adds value to the customer if it reduces the risk profile in a cost-effective and sustainable manner. Corrective, preventative and procedural improvements can be measured through the integration of security performance measurement metrics that are directly linked to the customer’s prevailing security risk profile.

Physical security as an organisational function should add intrinsic value to the customer’s business/organisation value chain. Security’s value should be measured against the reduction of risks through loss prevention, protection and recovery of customer assets. The SMC’s services should be measured in similar terms once mutually agreed.

For more information contact Physical Risk, +27 (0)12 851 2963, info@physicalrisk.com, www.physicalrisk.com
THE ULTIMATE MEETING PLACE FOR AFRICA’S LEADING SECURITY AND FIRE PROFESSIONALS

18-20 June 2013 at Gallagher Convention Centre Johannesburg, South Africa

IFSEC South Africa
COMMERCIAL & GOVERNMENT SECURITY • FIRE

18-20 June 2013, Gallagher Convention Centre
Johannesburg, South Africa

As the biggest exhibition of its kind on the African continent, IFSEC South Africa has a history dating back 19 years as the premier event that brings the entire security and fire industry supply chain together under one roof. IFSEC South Africa 2012 attracted 5,902 visitors from the government, trade and end-user market – all eager to seek innovative products and meet new suppliers.

IFSEC South Africa 2013 will include the launch of a dedicated Fire Pavilion, providing those exhibitors that specialise in fire safety products and solutions.

The IFSEC South Africa 2013 Fire Pavilion will provide an unsurpassed opportunity for visitors to see and compare the widest range of innovative fire solutions while networking with industry experts from all aspects of fire safety.

Homeland Security and Safety Africa is a dedicated Exhibition Zone and Conference at IFSEC South Africa. Aimed at delegates representing various government departments in Africa, Homeland Security and Safety Africa provides visitors and delegates with a direct link to these exhibitors showcasing their top products and services for national security. It features companies that assist both government and organisations with national resilience, counter-terrorism, border security, national surveillance and policing issues.

For more information visit www.ifsecsa.com or contact us directly

Charlene Hefer – Key Accounts Manager
T: 011 835 1565
E: charleneh@specialised.com

Do Wet Huysamer – Sales Executive
T: 011 835 1565
E: deweth@specialised.com

Ross Cullingworth – Portfolio Director
T: 011 835 1565
E: rossc@specialised.com

Co-located with:

OSH EXPO Africa
HOMELAND Security and Safety Africa

Official Media Partner:
hi-tech Security solutions

Organised by:
UBM MONTGOMERY
ZKTeco: new name, new opportunities

ZKSoftware is well known in South and southern Africa as a supplier of access control and T&A products, both card and biometric based. This successful Chinese company has carved a significant share of the local market since it first launched its local operation in 2005. Hendrik Combrinck, who together with his team has made the company a household name in the access control and T&A industry over the past several years, heads the local office since 2009.

Towards the end of 2011, the global ZKSoftware holding company restructured to be able to expand its fields of operation and ensure it delivers the optimal service to customers in order to back up its product range. The holding company is now known as ZKTeco. Combrinck says ZKTeco has been divided into five divisions, each with a specific focus area. They are as follows:

**ZKAcess**: ZKAcess is now responsible for the company’s access control products, from access control panels through to IP-based standalone RFID devices and Wiegand RFID slave readers. This division will also handle ZK’s biometric and facial access systems, as well as accessories for these devices.

**ZKSoftware**: The ZKSoftware division is responsible for the company’s time & attendance applications as well as the associated hardware.

**ZKBiologic**: ZKBiologic will concentrate on card, proximity and biometric door locks, especially focusing on the hotel and retail industries.

**ZKiVision**: ZKiVision is a brand new operation for ZKTeco that has already been launched in South Africa. ZKiVision will now distribute a range of 1 megapixel (720p) IP cameras along with camera management software. Combrinck says the division has four flagship camera ranges available in South Africa at present, and these will expand over time.

The unique selling point of the camera range, according to Combrinck, is the software. Customers will find the standard camera management software on their devices, but this is upgradable to software that integrates with access control products and can even do facial recognition on the camera. The access control integration will ensure that if a door is forced, for example, the camera will automatically record the incident without being told where to focus or what to do.

**ZKAFIS**: The ZKAFIS (automated fingerprint identification system) division is the newest division of ZKTeco, which will be launching its product line in early 2013. This will include matching server software for integrators who wish to build AFIS for Civil ID and Commercial ID projects.

For more information contact ZKTeco (SA), +27 (0)12 259 1047, hendrik@zkteco.co.za

It will also offer fingerprint modules to safe manufacturers and other industries that are interested in integrating biometric locks into their solutions.

**ZKAFIS**: The ZKAFIS (automated fingerprint identification system) division is the newest division of ZKTeco, which will be launching its product line in early 2013. This will include matching server software for integrators who wish to build AFIS for Civil ID and Commercial ID projects.

For more information contact ZKTeco (SA), +27 (0)12 259 1047, hendrik@zkteco.co.za
ZKTeco

Explore. Dream. Discover

www.zkteco.co.za

inBio160 - 1 Door with F12 Fingerprint Readers

inBio260 - 2 Doors with F12 Fingerprint Readers

inBio460 - 4 Doors with F12 Fingerprint Readers

inBio
Biometric
Control Panels

C3 Proximity Control Panels

C3-100 (1 Door)
C3-200 (2 Doors)
C3-400 (4 Doors)

REGAL
Your One Stop Security Shop

www.REGALSECURITY.co.za

AVAILABLE NATIONWIDE

HEAD OFFICE
9 Electron Street, Linbro Business Park,
Marlboro Drive, Sandton
Phone: (011) 553 - 3300
Putting its money on integrated security

Micro-finance company protects staff and assets with integrated security solution.

With more than 400 employees in its 80 plus branches, all of which hold large sums of money on site, Barko Financial Services needed a highly advanced security system to protect its people and premises.

Aware of the limitations of a one-size-fits-all system, the company approached Elvey Security Technologies to find a solution for its complex security needs, says Vic Marnewick, technical manager for Barko Financial Services.

One of South Africa’s leading micro-finance companies, Barko provides credit to millions of modest-earners throughout South Africa. It currently operates in five provinces (Mpumalanga, Gauteng, Limpopo, North West and KwaZulu-Natal), with its central monitoring station located in Pretoria.

“The DSC 1864, which was installed in all the branches, provides impressive levels of security as a result of its support of wireless IP communication as well as applications such as wireless communicators and office automation. It also offers a 500-event buffer, programmable night zone, automatic Contact ID and partitionable auto-arm timer.”

The solution to Barko’s communication problem was arrived at through the DSC TL250, a communicator that allows for redundancy signals to be sent to the control room via an IP line. Data transmissions created by TL250 IP alarm communicators are small and require very little network bandwidth, which ensures instant, reliable and accurate delivery of signals.

Explains Marnewick: “Barko Financial Services is a large operation which is vulnerable to theft, robbery and fraud owing to the presence of large amounts of cash on the premises. We therefore required a highly specialised, customised security solution that would ensure the protection of our employees, clients and property.”

The system had to meet a number of challenges. Firstly, the company’s central monitoring station had to be able to deal with alarm signals originating from all over the country. “Should our Polokwane branch experience an alarm, for instance, we had to be able to handle it in Pretoria since our branch managers are not allowed access to the alarm panel logs. Only our security supervisors have access to them, in order to protect the integrity of the logs,” says Marnewick.

Another issue was the company’s alarm panels. Programmed to communicate with the control centre via GPRS, signal transmission over the public network was unreliable. He explains: “We were particularly concerned about signal failure in an emergency such as an armed robbery since our control room operators would be totally blind and accordingly unable to render timeous and appropriate assistance.”

Further to this, Barko needed to address its control room’s inability to receive live feeds from branches. “We have to have our eyes on all our branches in order to be able to monitor situations as well as catch dishonest clients and staff,” he says.

Effective solution

After consulting with security systems expert Leon Le Roux, a senior member of the Elvey team, the decision was taken to install an advanced in-house surveillance, monitoring and communication system that would springboard off DSC’s new 1864 alarm panel. Explains Le Roux:

“The unit offers excellent functionality,” says Marnewick. “For one, it can report to two different IP addresses, which means it doesn’t go down even if the primary receiver IP address becomes inaccessible. For another, our security staff can extract event logs over the Internet from the comfort of the control room without them having to drive or fly to the branches.”

The system’s CCTV component makes it possible for Barko Financial Services to monitor all its branches via the click of a button. Smaller branches were fitted with 4-channel DVRs while larger branches received 8- or 16-channel DVRs, all boasting built-in Web servers. “This feature makes it possible for us to access live footage from any camera on the system from the control room,” he says.

The cameras provided by Elvey boast features such as high resolution 420TV Lines and 0.1Lux for low light level imaging. They also offer an onboard array of functions such as white balance, automatic gain control and backlight compensation, according to Le Roux.

More than alarms

“This is an incredible system,” says a delighted Marnewick. “Since its installation, we haven’t missed an alarm communication or signal. What’s more, staff members no longer have to waste company money and time travelling to the branches to retrieve event logs – they now download them in our control room.”

He concludes: “We’re also impressed with the functionality of the CCTV component of the system which not only allows us to monitor our branches remotely but, as a result of its facial recognition application, makes it possible for us to highlight suspicious characters and obtain vital evidence that can be used in court.”
### System integrators

It takes appropriate knowledge and experience to create solutions that protect people, profits and assets and deliver business benefits. Skilled, experienced system integrators are the link between technology and solutions that work.

As a service to our readers, Hi-Tech Security Solutions provides a list of system integrators end users can contact to discuss their integrated security solution requirements.

For details on how to include your company in this listing contact vivienne@technews.co.za

<table>
<thead>
<tr>
<th><strong>Bidvest Magnum</strong></th>
<th><strong>EOH Intelligent Infrastructure</strong></th>
<th><strong>Card Control Systems</strong></th>
<th><strong>Firetech Projects</strong></th>
<th><strong>Camsecure</strong></th>
<th><strong>Honeywell Building Solutions</strong></th>
<th><strong>UTM Group</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>We design, install and maintain integrated security solutions. As client requirements are unique, Bidvest Magnum Technology does not have off-the-shelf security solutions. Instead, we analyse the client’s needs, advise on optimum solutions, design the required system and then install it based on clearly defined project guidelines as well as a detailed scope-of-work document.</td>
<td>EOH Intelligent Infrastructure is a wholly owned subsidiary of EOH, and is responsible for sales, installation and support of products on the African continent. EOH Intelligent Infrastructure supplies and installs security, CCTV, access control, communications and time management solutions, building management, fire detection and offer a range of leasing solutions.</td>
<td>We provide total project solutions based on specialist design, engineering and maintenance services. CCS can design and install systems to suit your needs and budget. And we can evaluate, upgrade, repair and maintain your existing system. Specialise in surveillance: access control and T&amp;A, fire detection: audio evacuation and public address, as well as parking control systems.</td>
<td>Firetech Projects provides project solutions to many sectors of the market, including government, universities, hospitals, shopping malls, national key points, financial institutions and the private sector. It specialises in fully integrated fire and security systems both nationally and internationally. We pride ourselves on quality expertise and experience in building asset protection.</td>
<td>A network surveillance and electronic security company that has completed many large and prestigious projects throughout the continent. We pride ourselves on quality, expertise and experience. Designing event-driven systems and centralising information through maps, priority alarms and embedding standard operating procedures to quickly prompt the operator to make the correct response.</td>
<td>Honeywell Building Solutions is a leading provider of end-to-end total security management services with integrated solutions. These include managed surveillance, access control, time and attendance, video analytics, data mining and meaningful business intelligence. UTM delivers security management services by taking your entire risk value chain into consideration.</td>
<td></td>
</tr>
</tbody>
</table>
| Tel: +27 (0)11 555 4949  
kevinm@bidvestmagnum.co.za  
www.bidvestmagnum.co.za | Tel: 0861 500 500  
Fax: +27 (0)11 844 3500  
www.eohii.co.za | Tel: +27 (0)11 907 3192  
cardcon@mweb.co.za  
www.cardcontrolsystems.co.za | Tel: +27 (0)12 667 2338  
firetech@firetech.co.za  
www.firetech.co.za | Tel: +27 (0)11 781 1341  
support@camsecure.co.za  
www.camsecure.co.za | Tel: +27 (0)11 695 8000  
servicebsza@honeywell.com  
www.honeywell.co.za | Tel: 086 022 2266  
info@utmgroup.co.za  
www.utmgroup.co.za |
| **Jasco Security Solutions** | **TVMS** | **Basix Group** | **Camsecure** | **Honeywell Building Solutions** | **UTM Group** |
| Jasco Security Solutions (incorporating Scafell and Multivid) designs, installs and maintains security technology solutions. The business possesses great depth of skill and experience, along with a true understanding of the security challenges faced by organisations of all sizes. Together with the Jasco Group’s expertise in the ICT and Energy sectors, we provide turnkey solutions. | Our solutions protect and enhance your investments and profits as well as reduce risk. We provide holistic security technology solutions that enable you to concentrate on your core business. From design, installation and maintenance to monitoring, TVMS offers peace of mind with value for money solutions and exceptional service delivery. | The Basix Group, security system integrators and solution providers with over 20 years’ experience, and a strong presence throughout RSA, serves government and private sector customers in the financial, transportation, commercial-industrial and infrastructure markets. Basix is the agent for March Networks, a global provider of intelligent IP video solutions. | Tel: +27 (0)11 210 3500 Head Office  
info@basixgroup.co.za  
www.basixtech.co.za | Tel: +27 (0)11 695 8000  
servicebsza@honeywell.com  
www.honeywell.co.za | Tel: 086 022 2266  
info@utmgroup.co.za  
www.utmgroup.co.za |
| Tel: +27 (0)11 894 7127  
kleroux@multivid.co.za  
www.jasco.co.za | Tel: 0861 867 8867 (TVMS)  
sales@tvms.co.za  
www.tvms.co.za | Tel: +27 (0)11 500 500  
www.securitysa.com |

---

**UTM Group**

UTM Group is a provider of end-to-end total security management services with integrated solutions. These include managed surveillance, access control, time and attendance, video analytics, data mining and meaningful business intelligence. UTM delivers security management services by taking your entire risk value chain into consideration.

Tel: 086 022 2266  
info@utmgroup.co.za  
www.utmgroup.co.za
Niehaus explained that the reader is preset via the cellular network to alert the user when he or she is approaching a specific, designated Geo Zone. Once in the designated Geo Zone, the reader will automatically be enabled and the employee can clock for time and attendance (T&A). Once the employee leaves the Geo Zone, the reader will go into lockdown mode until the employee arrives in a new designated Geo Zone. The reader is also ideal for construction and mining companies where limited communications infrastructure exists.

By incorporating the EOH Cloud solution platform, all S-QUBE biometric devices are hosted, allowing clients direct access to a comprehensive workforce management solution with limited infrastructure expenses.

For more information contact EOH Intelligent Infrastructure, 0861 500 500, sales.ii@eoh.co.za, www.eohii.co.za

Android platform-based biometric reader

EOH Intelligent Infrastructure has developed the S-QUBE biometric reader.

Niehaus explained that the reader is preset via the cellular network to alert the user when he or she is approaching a specific, designated Geo Zone. Once in the designated Geo Zone, the reader will automatically be enabled and the employee can clock for time and attendance (T&A). Once the employee leaves the Geo Zone, the reader will go into lockdown mode until the employee arrives in a new designated Geo Zone. The reader is also ideal for construction and mining companies where limited communications infrastructure exists.

By incorporating the EOH Cloud solution platform, all S-QUBE biometric devices are hosted, allowing clients direct access to a comprehensive workforce management solution with limited infrastructure expenses.

For more information contact EOH Intelligent Infrastructure, 0861 500 500, sales.ii@eoh.co.za, www.eohii.co.za

EOH Intelligent Infrastructure has developed the S-QUBE biometric reader, using Morpho biometric technology, incorporated onto an Android platform. According to the company’s national sales manager, Freddy Niehaus, this is the first reader of its kind to offer the flexibility required in mobile and remote site workforce management solutions. The Android platform allows flexibility in design and opens new horizons for workforce management solutions. With its various wireless capabilities, it is ideal for use in areas where network installation is difficult or where network infrastructure costs need to be reduced. The resultant savings on maintenance of networks are also an attractive benefit.

In addition to the fact that this is one of the first locally designed biometric readers to operate on an Android platform, the new reader also incorporates GeoTagging. “This is highly advantageous for accurate timekeeping of employees, specifically with regard to those employees who travel a lot,” said Niehaus.
Jasco Security upgraded the security and access control systems at an upmarket residential and golf estate in northern Johannesburg, to cater for the daily influx of thousands of residents and visitors.

Jasco Security was contracted to design, supply, install and integrate the entire upgrade solution as well as to install new infrastructure, including new cables for the existing cameras, access control units, booms and pedestals, as well as pedestrian routes. The upgrade included moving from a card reader to a biometric solution as well as a migration from analogue cameras to an IP-based CCTV solution.

The project included vehicle access points, door access control, networking equipment and switches, wiring, slewing and connectors, static cameras at access control points, a video management system with hardware and software, storage and video recording management tools, customisation of the access control solutions as well as third-party integration between existing hand-held scanners and the upgraded system, and all civil work involved in laying of new cabling and construction of new aesthetically pleasing bollards for the biometric scanners.

Because of the high volumes of traffic and the nature of the estate, the estate required a robust CCTV solution that enables day/night visibility, along with Morpho biometric access terminals. These solutions integrate seamlessly and deliver a stable, reliable and highly secure environment.

The installation had to be conducted without hindering the existing security and access control and to minimise disruption to the residents and security guards during the project. This entailed working on one section at a time, and the final stage involved configuration and changing over the database from card to biometric and cutting over from analogue to IP cameras, and then integrating the solutions for a seamless user experience.

Other constraints during implementation included the need to preserve existing curbs, maintaining the aesthetic appeal of the Estate’s entrance and exit points, and constraining noise levels during certain hours of the day and on weekends.

For more information contact Jasco Security Solutions, +27 (0)11 894 7127/8, mmare@multivid.co.za, www.jasco.co.za
Flexible real-time system for a Massmart chain company

Offsite and onsite real-time retail video data analysis system for 12 stores.

The UTM Group is currently rolling out an offsite and onsite real-time retail video data analysis system to 12 stores within the Massmart chain group of companies. This is believed to be the only installation of its kind in southern Africa.

The installation incorporates a live IP access link from the retail stores' scanners and scales to the UTM Group's offices. According to Group MD, Kelly McIntock, each point where data is gathered is directly linked to UTM in order to ensure full optimisation of the system's capabilities.

UTM staff members are on site to provide technical backup. A data feed runs around the clock via IP, with IP video, including video analytics, being utilised both on- and offsite for security, merchandising, receiving management, SOP management and occupational health and safety.

Each installation will include between 38 to 60 cameras. UTM chose to use a customised blend of brands, for the head-end cameras in order to cater to the specific needs of each location and store.

Data mining by UTM allows the company to pinpoint problem areas within the stores and feed real-time information on incidents back to the store, as well as regional and executive management. The reports include comprehensive details of the location of the incident, a description of the incident (for example, cashier committing fraud to the value of R2.00; or shelving stock layout incorrect), as well as the time and frequency of the incident.

UTM selected the well-known Encanvas framework from the United Kingdom to handle all the middleware processing and data crunching and Chase, a South African homegrown PSIM (physical security information management) platform for incident management.

For more information contact UTM Group, 0860 22 22 66, Kelly@utmgroup.co.za

You can bank on this solution

One benefit of a converged network is that there is just one network to manage.

When a major financial institution went to tender for its new building, with a view of upgrading its security system, convergence into the company's IT infrastructure was one of the requirements. One benefit of a converged network is that there is just one network to manage. With separate voice, video, and data networks, changes to the network have to be coordinated across networks. There are also additional costs resulting from using three sets of network cabling. Using a single network means you just have to manage one wired infrastructure.

Bidvest Magnum's was the successful integrator and the design allows both the security system and the data network to run over the same infrastructure through the implementation of quality of service. In addition, the client requested the implementation of smart cards that would allow employees to transact in a virtually cash-free environment. Access for photocopying and payment for food and beverages at the canteen are now facilitated by using the Crescendo 1100 cards.

When visitors plan to visit the building a unique reference number is sent to them via SMS or e-mail. They then enter this reference number into the console at the remote kiosk and their photograph is taken. The system sends a link to the visitor's host and the visitor is then permitted to enter the building. This eliminates the need for a help desk in the reception area.

The scope of work includes the supply and installation of the EBI Temaline access control readers from Honeywell, Milestone open platform software, which allowed the client to be product agnostic on all security peripherals, thus allowing them to install various IP cameras manufactured for specific purposes, speed stiles integrated into the EBI access system, X-Ray devices and IP intercom systems. The project is due for completion in March 2013.

For more information contact Bidvest Magnum Technology, +27 (0)11 555 4949, kevinm@bidvestmagnum.co.za
Product highlights of 2012

What were the products from 2012 that we should be remembering?

Looking back over the past year, there have been a host of products released. And while it is Hi-Tech Security Solutions’ job to announce the various new products on the market (obviously we can’t cover them all), we thought the January issue would be a great time to highlight a few that stood out from the masses.

We asked our vendors to nominate products from their stable that stood out for them in the past year. We didn’t just want any product, but something that made a difference either in user demand or marking an inflection point for the company, a vertical or the market the technology was aimed at.

What follows is a few of the product highlights we received. It’s important to note that these are not products voted as “Best of 2012” by the end user, but rather product the vendors feel made an impact during the year and were well received by their customers.

**Product: CX702**
Manufacturer/Vendor: OPTEX
Distributor/Supplier: Elvey Security Technologies

Designed to render super-reliable detection on commercial premises, the CX702 passive infrared detector is ideal for wide angle and long-range applications.

**Motivation:**
According the Tinus Jansen van Vuuren, regional branch manager for Elvey, the CX702 is the product of choice among installers tasked with protecting commercial environments. Easy to install, reliable and effective, the feature-rich detector boasts multi-focus optics, spherical lens design, patented double conductive shielding, dual purpose lens, temperature compensation circuit and disturbance-free tamper switch. For sites requiring 24 m - 45 m long-range and 12 m - 21 m wide-angle protection, there’s nothing on the market to touch its performance.

Contact: Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za

**Product: CatVision Core**
Manufacturer/Vendor: Cathexis Technologies
Distributor/Supplier: MASS Solutions, Compass Life Safety, Cathexis Africa

The Cathexis Core Software is video management software that is ideal for small to medium solutions of up to 36 cameras. This product provides a low cost, yet sophisticated solution for multiple applications. This product is 100% locally developed and supported.

**Motivation:**
The Cathexis CatVision Core software has the flexibility to provide sophisticated surveillance for a range of needs, be it for individual single server sites or a multi-site enterprise. The CatVision Core software package is ideal for small to medium installations, whether the client is a small business with a single server or a larger enterprise with multiple outlets that requires centralised site management.

The open architecture enables IP or analogue cameras, recording and viewing servers as well as third-party systems (e.g. access control, fire panels, point-of-sale) suited to a particular application to be integrated seamlessly, thereby providing clients with the best solutions and maximum return on investment.

Technical “health monitoring” provides pro-active technical notifications as well as status reporting via e-mail and/or SMS.

Contact: Gus Brecher, Cathexis Africa, +27 (0)31 240 0800, info@cat.co.za

**Product: DH-SD6982A-HN**
Manufacturer/Vendor: Dahua Technology

- 2 MP full HD network IR PTZ dome camera with in-house block camera
- H.264 & MJPEG dual-stream encoding and JPEG image capture
- Max 25/30 fps @ 1080p
- Micro SD memory, IP66
- IR LEDs to 100 m

**Motivation:**

Contact: Dahua Technology, +86 571 8768 8883, overseas@dahuatech.com

**Product: MultiBio700**
Manufacturer/Vendor: ZKTeco
Distributor/Supplier: Accsys

Biometric access control device

**Motivation:**

You can have multiple access control in a single device. As the name would suggest the MultiBio700 is manufactured with four verification modes namely, facial verification, fingerprint verification, RFID proximity and PIN code. With a 3-inch colour touch screen and infrared camera, the MultiBio700 will fit in perfectly in any access control environment. The stylish design also enhances the ambience of the room or office.

Contact: Accsys, +27 (0)11 719 8000, pr@accsys.co.za, www.accsys.co.za
Product: **ZKS4**  
Manufacturer/Vendor: ZKTeco  
Distributor/Supplier: **Regal**  
Biometric access control device  
**Motivation:**  
The ZKS4 is manufactured with a robust steel housing and is an IP54 rated biometric access control device, with options of fingerprint or RFID card verification. The “eyelid” protecting the sensor is a unique feature protecting the unit from direct sunlight or bright light, making the reading capabilities easier and accurate. The ZKS4 has a standard TCP/IP communication and also a USB hub to manually download transactions. The ZKS4 is an extremely reliable product and very popular in the market.  
Contact: **Regal Security Distributors**, +27 (0)11 553 3300, sales@regalsecurity.co.za

Product: **S900 GPRS**  
Manufacturer/Vendor: ZKTeco  
Distributor/Supplier: **ERS Biometrics**  
Biometric time & attendance device  
**Motivation:**  
ERS has established itself in the market with the S900 GPRS device, due to the reliability and speed of the S900. The S900 has the capacity of 8 000 fingerprint templates and works seamlessly on the GPRS network making this a unique mobile device operating within the cloud solution. The elegant design of the S900 is complimented with a 3-inch full colour screen giving the client the unique ability of advertising company logos or displaying greeting messages. The speed of the device is powered by the latest ZK technology hardware enabling an increases in clocking’s and functionality.  
Contact: **ERS Biometrics**, +27 (0)10 593 0593, sales@ersbiometrics.co.za, www.ersbiometrics.co.za

Product: **DH-NVR3204/3208/3216-P**  
Manufacturer/Vendor: Dahua Technology  
• 4/8/16 channel 1U PoE NVR  
• H.264/MJPEG dual codec decoding  
• Max 120 fps @ 1080p, 240 fps @ 720p, 480 fps @ D1 preview & recording  
• Support multi-brand network cameras: Dahua, Arecont Vision, AXIS, Bosch, Brickcom, Canon, CP Plus, Dynacolor, Honeywell, Panasonic, Pelco, Samsung, Sanyo, Sony, Videosec, Vivotech and etc.  
• ONVIF Version 2.0 conformance  
• 3D intelligent positioning with Dahua PTZ camera  
• Support IPC UPnP, 4 PoE ports  
• Multiple network monitoring: Web viewer, CMS (DSS/PSS) & DMSS  
Contact: **Dahua Technology**, +86 571 87688883, overseas@dahuatech.com
SONY vandal-proof dome

- **Product:** SONY vandal-proof dome
- **Manufacturer/Vendor:** Trend Tech
- **Distributor/Supplier:** Crown Hyper World
  - Sony/CCD
  - 23 PCS LED
  - Vandal Resistant IP65
  - IR distance 20M
  - Usable illumination: 0.8 Lux (infrared lamps turn on)

**Motivation:**
- Vandal-resistant IP65
- Usable illumination: 0.8 Lux (infrared lamps turn on)
- Sony 520TVL

**Contact:**
Crown Hyper World, +27 (0)11 830 1452,
sales@crownhyperworld.co.za

---

Hamster

- **Product:** Hamster iDU5 & iPB6
- **Manufacturer/Vendor:** iPulse Systems
- **Distributor:** Elvey Security Technologies

**iPulse’s USB fingerprint readers,** which use the latest in patented SEIR technology, **have raised the bar in the field of fingerprint biometrics.**

**Motivation:**
- Used predominantly in stand-alone biometric access control applications, iPulse’s range of readers boast user-friendly software.
- Tried and tested, the entry point iDU5 reader meets the most exact standards of reliability and cost effectiveness. The iPB6 reader is a world-leader, with technology far ahead of its competitors. Unlike previous-generation biometric devices, the iPB6 is based on a Linux operating system. This makes it extremely versatile, able to run multiple business applications and perform a host of specific tasks.

**Contact:**
Elvey Security Technologies, +27 (0)11 401 6700,
info@elvey.co.za

---

When it comes to console design

- ProGroup designs command centre consoles to suite your specific needs.
- We design and install your console on time.
- Our consoles are made from rugged, scuff-proof materials.
- All consoles are designed to accommodate all requisite hardware.
- Consoles are designed to fit in with an existing design theme.
- The console can be created using a combination of materials from wood veneers and laminates to melamine, solid woods and more.

**the choice is yours.**

Call (011) 493 1545 or email us at sales@progroup.co.za
www.progroup.co.za
Product: CatObserver
Manufacturer/Vendor: Cathexis Technologies
Distributor/Supplier: MASS Solutions, Compass Life Safety, Cathexis Africa

The CatObserver product is a monitor recording add-on to the Cathexis CatVision software suite of products. This software enables one to easily stream one or more PC monitor views as if they were IP cameras.

Motivation:
The CatObserver enables the recording of any monitor connected to any Windows based system on a site network. Think of an operator following a suspect via multiple cameras on his spot monitor, and then a manager wanting to archive or review the cameras in question. In the past, one would need to know exactly which cameras were viewed, and then each individual camera accessed and viewed/archived at the relevant recording time. A tedious process.

With CatObserver, this is easy. All you have to do is to view/archive the channel associated with the operator’s monitor, and all the cameras that were viewed are accessed automatically. The software can also be used to stream point-of-sale or other data without having to complete a sophisticated integration with the third-party system.

Contact: Gus Brecher, Cathexis Africa, +27 (0)31 240 0800, info@cat.co.za

Product: EntraPass Web
Manufacturer/Vendor: Tyco Security Products
Distributor/Supplier: Tyco Security Products

EntraPass Web is a Web user interface that provides remote access from a mobile device to your EntraPass security management software. EntraPass Web provides access to a vast variety of access management tools, enabling anywhere, real-time management of all EntraPass security tasks.

Motivation:
Using any workstation connected to the Internet, EntraPass Web gives users the ability to control their EntraPass security system, including functions such as diverse operations, configurations and hardware setup functionalities, managing users and creating cards, and controlling access levels, schedules, holiday and tenant management. Users can also manage events, access floor plans and maps, as well as doors, relays, inputs, reports and many more functions. Built on EntraPass v5.03, EntraPass Web features a new user-centred design that is simple and efficient to use and is flexible and adaptable to changing user needs.

Contact: Ernest Mallett, Tyco Security Products, +27 (0)87 150 2990, emallett@tycoint.com

Product: Illustra 600 Series
Manufacturer/Vendor: Tyco Security Products
Distributor/Supplier: Tyco Security Products

The Illustra 600 Series HD IP mini-dome cameras offer facial detection capabilities and auto-focus lenses, which enables zoom adjustment and auto-focus control via the Web interface. The cameras offer HD video quality in all lighting conditions and are ONVIF compliant.

Motivation:
The Illustra 600 series cameras can detect a face and increase the bit rate around it without cropping out background images, saving on bandwidth and storage costs. This technology reduces energy demand for the whole system, due to the reduced amount of data. Face detection can be used indoors or outdoors where high-resolution images of faces are essential to security such as bank lines, cash registers, stairwells and entrances and exits. Designed for integrators and end users interested in the ability to automatically detect faces and enhance a ‘region of interest’ in a live scene, such as for retailing, gaming and banking.

Contact: Ernest Mallett, Tyco Security Products, +27 (0)87 150 2990, emallett@tycoint.com

Product: Intevo
Manufacturer/Vendor: Tyco Security Products
Distributor/Supplier: Tyco Security Products

Intevo is an easy to deploy, integrated security system, supporting Web and mobile clients, control for access readers and management of networks of up to 32 IP cameras. Intevo is preconfigured for intrusion and preloaded with Kantech’s EntraPass software and American Dynamics’ IP video recorder.

Motivation:
The Intevo is a single appliance featuring integrated access control, video and intrusion, designed to be up and running in minimal time with out-of-the-box ease. With the included first boot wizard, Intevo is simple to configure and a customised dashboard provides seamless navigation among software applications. This results in a single user interface, greatly simplifying security management functions for users, making it ideal for both small and large projects. Intevo provides a platform for small to medium businesses as well the ability to grow the system to meet organisational needs over time.

Contact: Ernest Mallett, Tyco Security Products, +27 (0)87 150 2990, emallett@tycoint.com
Product: TX-SMS
Manufacturer/Vendor: Radio Data Communications (RDC)
Distributor/Supplier: Elvey Security Technologies
Compatible with all major alarm control panels, the sleek design of this SMS communicator is complemented by a host of impressive features, including full Ademco Contact ID reporting to cell phones.

Motivation:
The popular outdoor infrared detector comes packed with a selection of settings and adjustments to allow for every conceivable application and environment. It’s stable, reliable and has multiple mounting options, all of which complement its core functionality: an early-warning system for homes and businesses.

Contact: Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za

Product: VX-402
Manufacturer/Vendor: Optex
Distributor: Elvey Security Technologies
The VX-402 is a multi-stabilised outdoor detector that takes commercial and domestic perimeter protection to new levels.

Motivation:
The popular outdoor infrared detector comes packed with a selection of settings and adjustments to allow for every conceivable application and environment. It’s stable, reliable and has multiple mounting options, all of which complement its core functionality: an early-warning system for homes and businesses.

Contact: Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za

Product: VX-402
Manufacturer/Vendor: Optex
Distributor: Elvey Security Technologies
The VX-402 is a multi-stabilised outdoor detector that takes commercial and domestic perimeter protection to new levels.

Motivation:
The popular outdoor infrared detector comes packed with a selection of settings and adjustments to allow for every conceivable application and environment. It’s stable, reliable and has multiple mounting options, all of which complement its core functionality: an early-warning system for homes and businesses.

Contact: Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za

Product: emerald
Manufacturer/Vendor: CEM Systems
Distributor/Supplier: CEM Systems
As one of the industry’s most multi-functional intelligent access terminals, emerald features a card reader and controller, a scramble keypad for PIN authentication, a built-in Voice over IP (VoIP) intercom and a range of remote server based applications, in one device.

Motivation:
As another industry first by CEM, emerald not only controls access to restricted areas, but opens up a world of possibilities by bringing security intelligence directly to the edge. emerald was designed with high security and flexibility in mind and provides users with a new access control experience.

Contact: Ernest Mallett, Tyco Security Products, +27 (0)87 150 2990, emallett@tycoint.com

Ideal for hotels, restaurants, office buildings, shops; but also for installation in devices like ATMs.

Hemispheric camera for concealed installation
Inconspicuous and elegant

NEW S14M

MOBOTIX S14M Features:
- Mono Hemispheric built-in camera for concealed installation
- With integrated on-board sensor
- 180 degree horizontal viewing angle
- 3 MP Video Resolution at 20 FPS
- Suitable for mounting behind a wall or ceiling
- Robust and maintenance-free, without moving parts
- Waterproof connectors
- Concealed Housing (IP65)
- Vandal Resistant
- Extra strength housing for protection against damage and vandalism
- Tamper Resistant
- Camera intelligence to detect and notify when tampering occurs
- Ruggedized
- Sturdy design that can withstand tough conditions
- Includes 4GB Micro-SD card

Security-Vision-Systems
IAC CONTACT DETAILS:
TEL: +27 (0)12 657 3600
FAX: +27 (0)12 657 3630
www.iaconline.co.za

MOBOTIX
World’s No.1 in High Resolution IP Video

CONVERGED COMMUNICATIONS
POLOphone

**Manufacturer/Vendor:** Centurion Systems
**Distributor/Supplier:** Keep Access Control Systems

POLOphone is an expandable intercom system. From a single function kit, components may be added to expand the system. POLOphone can accommodate up to four handsets with single entry panel or three handsets with two entry panels. Intercommunication between handsets is possible.

**Motivation:**
The POLOphone is an affordable expandable intercom system. From a basic single kit, it can be expanded into an ideal system for larger houses or small office installations. POLOphone can accommodate up to four handsets with a single entry panel or three handsets with two entry panels each. Intercommunication between groups of handsets adds to the POLOphone's versatility and value for money.

Installation is simple, requiring a 2-wire bus throughout, to which entry panels/phones may be connected at any point. A low current 12 V DC power supply allows for the system to be connected to the battery of a Centurion gate motor for power failure protection.

Contact: Keep Access Control Systems, +27 (0)11 805 0175, esales@keepacs.co.za

Sector

**Manufacturer/Vendor:** Centurion Systems
**Distributor/Supplier:** Keep Access Control Systems

A boom system with custom built DC motor and gear box, can raise up to a three metre boom pole in less than 1.2 seconds, or a six metre pole, smoothly and reliably, at a slightly lower speed. Features include onboard Nova rolling code, integrated ChronoGuard timer functionality and multi-channel receiver.

**Motivation:**
The Sector is designed for tough, high volume usage and is built to endure millions of cycles. An important feature is full battery backup to ensure uninterrupted access during power outages. Setup is kept simple with the use of a user-friendly LCD user interface. The boom pole operates at high torque, with smooth, intelligent speed control. The onboard rolling code uses Keeloq encryption and the multi-channel receiver includes a selective delete function.

With its slimline operator casing and set-up versatility, the Sector offers a speedy, effective and reliable access control solution.

Contact: Keep Access Control Systems, +27 (0)11 805 0175, esales@keepacs.co.za

IN01-A

**Manufacturer/Vendor:** ZKTeco
**Distributor/Supplier:** EOHii

Biometric time & attendance with access control device

**Motivation:**
If its loyalty you want, the IN01-A is just the product. The IN01-A has proven itself through the years to be a reliable and a stable time and attendance device. Included in this device is the option to add access control, with the built-in relays. Standard functions on the IN01 include: colour screen, integrated 125 kHz RFID proximity and capacity of 3 000 fingerprint templates. Notable is the feature of a built-in battery backup.

Contact: EOHii, +27 (0)11 844 3200, siresen.naidoo@eoh.co.za, www.eohii.co.za

16-channel DVR

**Manufacturer/Vendor:** Trend Tech
**Distributor/Supplier:** Crown Hyper

High-speed CPU 400/600MHz, 2GB memory space, flash 16 MB with excellent GUI display. H.264 main profile video compression enhances 2.2 times of image quality and reduces 40% HDD occupation space. Dual encoding streams support. Linux operation system with D1 high resolution.

**Motivation:**
Dual encoding streams support D1/2CIF/CIF/QCIF resolution programmable. Support for 1080P HDMI output optional, genuine HD VGA output and BNC output at the same time, 4/8/16 CH video loop out optional. Support for DHCP/PPPOE/FTP/DNS/DDNS/NTP/e-mail alarm/IP right management/IP search/network alarm centre functions, support Web client, standalone client and SDK.

Contact: Crown Hyper, +27 (0)11 830 1452, sales@crownhyperworld.co.za
Product: PowerMaster-30 G2
Manufacturer/Vendor: Visonic / Tyco Security Products
Distributor/Supplier: Tyco Security Products
A professional wireless security, safety and control system based on Visonic’s PowerG technology, PowerMaster-30 G2 incorporates visual verification, advanced applications and is suitable for the noisiest wireless environments with superior range, prolonged battery life and unmatched wireless robustness.

Motivation:
PowerMaster-30 G2 is based on technology from Visonic called PowerG, combining design elements from Bluetooth (e.g. Frequency hopping), Cellular (e.g. TDMA, Auto-Power-Adjustment), etc. The combination of these elements create a modern wireless network which works on dry cell batteries for 5 to 8 years, while still maintaining 2-way communication between the control panel and the devices.

PowerMaster panels enable advanced applications such as camera-based applications, configuration of detectors from panel menus and continuous monitoring and diagnostics of wireless connections. PowerMaster also assists installers in finding optimal mounting spots, or locating a problematic device amongst many similar devices in the room.

Contact: Ernest Mallett, Tyco Security Products, +27 (0)87 150 2990, emallett@tycoint.com

Product: Registers
Manufacturer/Vendor: RBE
Distributor/Supplier: RBE
RBE manufactures and distributes two widely used security entry control registers tailored for the residential/estate security market.

Motivation:
Occurrence Books and Gate Entry Control Books are the most commonly used registers. These books are available as an ex-stock standard item, or, can be designed and printed to the security company’s specific requirements with logo.

Contact: RBE, +27 (0)11 792 7321, sales@rbe.co.za

Product: CatVision Premium
Manufacturer/Vendor: Cathexis Technologies
Distributor/Supplier: MASS Solutions, Compass Life Safety, Cathexis Africa
The Cathexis Premium Software is a high-end video management solution that is designed for large to very large sites or multi-site enterprise IP or hybrid video solutions. The system provides unlimited cameras and servers and viewing/management users as well as sophisticated third-party integration capability. This product is 100% locally developed and supported.

Motivation:
The Cathexis CatVision Premium software provides an integrated surveillance solution of unlimited functionality and scale for large sites or multiple site population. This top of the range feature-rich software is ideally suited to the mining environment, major industrial sites, airports, city surveillance and many other situations that require very large camera populations with complete multi-tier management control.

The open architecture enables unlimited numbers of IP and analogue cameras, recording and viewing servers as well as third-party systems suited to a particular application to be integrated seamlessly, thereby providing clients with the best solutions and maximum return on investment.

Technical “health monitoring” provides pro-active technical notifications as well as status reporting via e-mail and/or SMS.

Contact: Gus Brecher, Cathexis Africa, +27 (0)31 240 0800, info@cat.co.za
SmokeCloak rapidly (within 30 seconds) floods an area under attack with a dense white harmless vapour and in so doing reduces visibility to approximately 15 cm making it impossible for the intruder to steal or attack anyone or anything.

**Motivation:**
SmokeCloak is a theft prevention product which has to be seen in action to be believed. It is undoubtedly the first security product that fights back effectively, driving the thugs away. SmokeCloak essentially buys time between an alarm activation and an armed response, and at the same time provides you with the safety of a place for you and your family to hide while you wait for help.

Contact: Transaction Control Technologies (TCT), 0861 SMOKEM (766536), sales@tct.co.za

---

**Product:** DH-IPC-HFW2100
**Manufacturer/Vendor:** Dahua Technology
- 1.3 MP HD network mini IR-bullet camera (20 m).
- H.264 & MJPEG dual-stream encoding.
- Max 15 fps @ 1.3 MP (1280×960) & 25/30 fps @ 720P (1280×720).
- 6 mm fixed Lens (3.6 mm, 8 mm optional).
- IP66, PoE.

**Motivation:**
- 1/3-inch 1.3 MP progressive scan Aptina CMOS.
- H.264 & MJPEG dual-stream encoding.
- Max 15 fps @ 1.3 MP (1280×960) & 25/30 fps @ 720P (1280×720).
- Day/Night (ICR), 2DNR, AWB, AGC, BLC.
- Multiple network monitoring: Web viewer, CMS (DSS/PSS) & DMSS.
- 6 mm fixed Lens (3.6 mm, 8 mm optional).

Contact: Dahua Technology, +86 571 8768 8883, overseas@dahuatech.com

---

**Product:** DH-SD6582A-HN
**Manufacturer/Vendor:** Dahua Technology
- 2 MP full HD network PTZ dome camera with in-house block camera
- H.264 & MJPEG dual-stream encoding
- Max 25/30 fps @ 1080p resolution
- Built-in 7/2 alarm in/out
- Easy installation with quick-installation port
- Micro SD memory, IP67

**Motivation:**
- 4.7 mm ~ 94.0 mm (20x) optical zoom
- H.264 & JPEG dual-stream encoding
- Max 25/30 fps @ 1080p resolution
- DWDR (Digital WDR), day/night (ICR), DNR (2D&3D), auto iris, auto focus, AWB, AGC, BLC
- Multiple network monitoring: Web viewer, CMS (DSS/PSS) & DMSS
- Max 400-degrees/s pan speed, 360-degree endless pan rotation
- Up to 255 presets, 5 auto scan, 8 tour, 5 pattern
- Built-in 7/2 alarm in/out
- Support intelligent 3D positioning with DH-SD protocol
- Micro SD memory, IP67, easy installation

Contact: Dahua Technology, +86 571 8768 8883, overseas@dahuatech.com

---

**Product:** Nova Loader
**Manufacturer/Vendor:** Comb Communications
**Distributor/Supplier:** Keep Access Control Systems

The Nova Loader is used to program remotes on the MKII system, by sending information to the website. It enables the quick and simple addition and deletion of remotes and PIN codes and the importing and exporting of spreadsheets, all performed online.

**Motivation:**
Once the Nova Loader is plugged into a USB port on the user’s computer, there is no longer any need to drive to the gate intercom to program remotes. Nova Loader sends all the relevant information to the website of the MKII system and all changes are performed on line, via a few keystrokes and a push of the remote button.

Remotes and users can also be selectively added to the MKII system or deleted, and PIN codes can be added, deleted or changed without any fuss. An additional feature which allows for the importing and exporting of spreadsheets ensures ease and quality of reporting.

Contact: Keep Access Control Systems, +27 (0)11 805 0175, esales@keepacs.co.za
CatVision Surveillance Solutions
Digital surveillance and beyond

Cathexis Setup Wizards

Our new Wizards make setting up our systems seem like Magic

email: info@cat.co.za

Download our IP Video Management Software FREE

www.cathexis.co.za
As safe as houses?
By Allyson Koekhoven.

How safe are our homes against the increasing criminal scourge?

Is the big security spending reserved for business installations or are residential owners wising up to the benefits of securing their properties? Hi-Tech Security Solutions asked three industry players about current trends in residential security.

Andre Mundell, independent security risk assessor at Alwinco, believes that residents and residents’ associations are not doing enough to protect themselves from criminals. “Unfortunately, in many instances, residents and residents’ associations blindly believe whatever the security salesperson tells them. “The perception is often that what sufficed as a security system in 1980 will be adequate today. Often, residents believe that an alarm system is an end in itself rather than a means to an end. The criminal modus operandi has become more sophisticated and people need to realise that a more comprehensive and integrated security solution is the only answer.

“Unfortunately, in many instances, residents and residents’ associations blindly believe whatever the security salesperson tells them.

“In general, there is little or no planning for security, with regard to both private residents and those living in estates and complexes. However, we are hopeful that this will change as residents and residents’ associations realise the benefits of implementing strategically planned installations.”

Louis Parker, CEO at ATEC Systems and Technologies is more optimistic about the uptake of adequate security systems. “We have witnessed a number of residents’ associations upgrading their card access control systems to biometric access control. Obviously, due to the costs involved, this is more prevalent in the upper LSM estates, but it definitely does not exclude all middle and lower LSM housing estates.

“The problems encountered with card access control systems include loss of cards as well as card owners giving their cards to third parties so that they can access the complex. The possibility of unlawful entry and probable criminal activity obviously increases in these instances,” Parker said.

Improved visitor management

“Fortunately, there seems to be a trend towards residents and residents’ associations becoming more proactive in terms of visitor management. The days of the security guard asking a visitor to sign in are fast becoming obsolete. The major problems with log books are that the writing is often illegible, information can be easily falsified, and information is difficult to track down retrospectively.”

Many of the residential estates are using hand scanners to scan the registration disk on the vehicle’s windscreen as well as the driver’s licence, while the more upmarket complexes are also utilising number plate recognition cameras. Live data can then be reviewed instantly rather than on an incident-only basis, as is common with visitor logbooks.

However, this is also a very big security risk as a means of access control. The problem this poses for security is that when the guards work with the scanner, they tend to concentrate on scanning the vehicle and licence and often don’t notice who is sitting in the vehicle or what is happening in the vehicle itself.

“The next problem we have with the scanner is knowing what happens with that information. Bear in mind that the guard now has your vehicle registration number as well as your ID number. Although some of the estates say that the information is password protected, the fact is that it is still available. It is critical that if you use handheld scanners, the security officers using them have the necessary security training and clearance to safeguard that information,” Mundell added.

Joe Naidoo, owner of Umvukele Security said that often the problem arises where a residents’ association contracts a number of different companies to supply their CCTV, access control, electric fencing and guarding needs. “It is preferable to contract one company to source, install and monitor all the solutions as a cohesive whole rather than ‘piecemealing’ each element.”

Parker said that in Gauteng his company has seen an increase in the number of security installations using integrated technology solutions, together with a guarding element, for a collaborative effort.

Security 101

“We find that often the decision-making and purchasing in residential complexes is left up to the secretary or a similar representative of the residents’ association. The danger here is that there is no accountability on the part of the individual residents. This is also apparent in the frequently encountered casual attitude that complex/estate residents have towards security. They tend to operate on the assumption that their neighbours will look out for their best interests,” Naidoo added.

“We have a saying that a complex is like picnic (or is that ‘pick-nick’?) basket – once the criminal gains access to the complex, he can pick
and choose which units he wishes to burglarise. Sadly, many residents in complexes and estates believe that, because the complex has a wall, electronic gate and a security guard, they and their possessions are safeguarded,” Mundell said.

“There is a desperate need for education of residents so that they can effectively protect themselves. They need to be made aware of their complex's weak spots and what systems can be implemented to mitigate the risks,” Mundell continued.

While all interviewees believe that the security options have changed in residential security, Mundell is not convinced that residents have kept pace with current offerings. “Unfortunately, the guard-plus-dog scenario seems to be the accepted norm for a number of residents living in residential estates and complexes. It is our duty as an industry to share the benefits of technology and also make residents and their relevant associations aware of what technology criminals are using to counter security technology.”

Education is key
“Awareness campaigns are driving consumers towards viable security solutions such as increased lighting, erecting walls and armed response. Popular amongst the higher income bracket residents is the ability to remotely monitor their property via their cell phone,” said Naidoo.

“Knowledge is king,” according to Mundell. “Residents and residents’ associations would be advised to consult with an independent risk assessor before making any decisions regarding their security. A credible risk assessor will determine what weak areas exist in a private residence as well as in a residential complex environment. One needs to bear in mind that the risk factor in a housing estate can be multiplied by two times the number of adults plus one person. Add children to the equation and you need to multiply the risk factor by six. This is due to the fact that children are often unaware of even the most obvious risks.”

Mundell cited a number of penetration tests he conducted when performing risk assessments. “The results were really quite scary. In most instances, I was able to get at least one of the residents to open the main security gate by using a futile reason for entry. In all instances, one needs to answer the question: ‘Is your will to stop a criminal greater than the criminal’s will to get into your property?’ You then need to follow through on your intent with strategic action.”

Package to fit your pocket
It is all very well proposing that residents and residents’ associations embark on risk assessments and implement comprehensive security solutions, but at what cost? While many of the upper LSM residential estates are able to afford benchmark technology, is this type of expenditure not beyond the budget of the average Joe?

All three interviewees agreed that communication with a service provider is critical and that systems can be customised to fit specific needs and budgets. Mundell said that the first step is to consider the area and the environment in which the residential estate or residence is situated. “Following the identification of risks is the appointment of an independent leader to guide and implement the security system. By employing a motivated person who has no alliance to the security provider, the best interests of the residents, rather than the interests of the service provider, are uppermost.”

“The crux of a solution could be merely changing the procedures around entry to the property by adding motion sensors or extra lighting. In terms of residential estates, residents could be told to turn all their lights on at night or suspect that criminal activity is taking place. In this way, everyone is on the same page and alerts to potential threats are concerted and timeous,” he elaborated.

In order to achieve maximum return on investment, Naidoo suggested that residents and residents’ associations ensure that the service provider can guarantee and prove that their guarding staff is accredited and disciplined. “Unfortunately, Security Officers Board certification is not enough to provide these guarantees. The service provider needs to ensure that his security officers receive adequate induction and training and that comprehensive background checks are performed on their employees.”

“Likewise, armed response personnel should receive training on procedures to follow when reacting to an alarm or callout. It is simply not enough that the reaction officer accepts the word of the ‘owner’ that everything is fine when he is responding to an event. Each situation should be approached as a possible duress incident and the response personnel should employ their resources to verify and validate non-events,” said Naidoo.

Mundell added that it is advisable for residents’ associations to prioritise security as an item on their agenda for meetings with residents. “Residents need to be made aware of the correct procedures to follow in terms of the use of panic buttons as well as receive updates on crime in their particular area. Forewarned is forearmed in this respect and the more information a resident has on the security systems in place within their residential estate, the more the likelihood of crimes being prevented or reduced.”

Warning!
The interviewees were asked what to avoid when considering a security system. Parker said that the first step is finding a reputable service provider. “Ask for references and ensure that they use well-known and supported brands. The service provider needs to supply a service level agreement (SLA) that outlines all elements incorporated in the system and includes the expected outcomes as required by the client.”

“Future upgrade capabilities are important in terms of technology. Your service provider should not be a jack-of-all-trades, but should rather bring in expertise in specific areas where required. Accreditation of service providers is important and a proper site survey will ensure that the proposed system can be motivated in terms of fit for purpose,” said Naidoo.

“Do market research and do not settle on the first service provider who knocks on your door. Conduct a risk assessment through an independent risk assessor to ensure objectivity. Avoid single-system (one-brand) solutions. Try to implement systems that allow the resident to access their residence via a cell phone or smart device,” Mundell outlined.

“In addition, from a physical and practical perspective, one should avoid dark areas and ‘hotspots’. By having an understanding of the criminal and what motivates them, you can employ avoidance systems. Finally, a system should be easy to use and activate otherwise it will have no worth,” he concluded.

Wireless estates
Peter Turvey, country manager for Radwin SA, says there are three primary reasons to look at using wireless networks in residential/estate security implementations:

1. Speed of installation,
2. You do not have to dig up roads and pavements, and
3. The costs of not having to do such earth works is substantial.

“Telco-grade wireless delivers everything that any video surveillance cabled system can, but with added benefits,” adds Turvey.
Security in home automation
By Brad Snaith, HomeIQ.

Is home automation the next horizon for security installers?

A key element of the modern smart home is its security system and there are a number of ways for contractors to tap into this lucrative market.

Intruder alarm installers today face a highly competitive environment. The market for intruder alarms, though large, is not growing as fast as it could do. Intruder alarm integrators typically offer CCTV, access control, automatic gates and intercoms as part of a total package.

The intruder alarms available are not highly differentiated, all typically offering the same features and capabilities with little consumer brand recognition. As a result, price competition in established markets is fierce as end users know that any alarm installation company listed in the phone book is likely to be able to offer a similar system. Home automation systems provide an alternative and an additional source of revenue that is readily accessible to electrical contractors who have developed their interest in smart home technology and its intruder alarm capabilities.

Home automation
The term home automation has been used in many contexts, from high-speed networks, computer controlled homes, universal remote controls, touch screens, lighting systems with scene control, home cinema and sound systems.

Home automation systems provide an alternative and an additional source of revenue that is readily accessible to electrical contractors.

Home automation is the ability to intelligently coordinate and monitor the operation and behaviour of appliances, lighting and subsystems in the home to achieve security, comfort, convenience and energy saving. The ability to use a remote control or touch screen or a designer keypad to control lights or a sound system is not an example of useful home automation. Such simple remote controlled systems just replace mechanical switches and have the benefit of convenience, but do little more. The ideal automated home would require very little direct intervention from the occupants except to make changes to its preferred behaviour from time to time, although this ideal does not fully exist at present.

A security system, or more accurately, an intruder alarm system is an essential part of most homes. Alarm systems typically have one or more keypads, magnetic sensors on external doors and windows and one or more motion sensors or passive infrared detectors (PIR’s) within the house. When the alarm system is armed, any intrusion detected by the sensors causes the sounders to be activated and perhaps the alarm monitoring company to be notified.

Many homeowners install security systems to obtain the benefits of lower insurance rates. However, the true benefits of home security far exceed any savings in insurance. When the alarm system is connected to a central home automation controller, or is part of a home automation system, then an intelligent home becomes possible.

A basic means of integrating security with lighting is the signalling of events from the former to the latter. Most simple alarm systems have a few outputs that are triggered by say, an intruder alarm or the system being armed and disarmed. In this manner, the lights can be made to switch on in the event of an alarm or to switch off when the system is armed. In a practical home automation system, it is only necessary to control strategic lights so that they can respond to predefined events.

Benefits
More sophisticated security systems are available that are well suited to act as the main controller in a home system or to communicate with another controller. Such systems have many programmable outputs as well as the ability to communicate via a serial interface like RS-232 or Ethernet to lighting and other third-party products. Events like the arming and disarming of the security system, movement in any zone, opening and closing of doors and windows and the occurrence of specific alarms like intruder, fire, and power failure can be linked to lighting and other subsystems in the home. This allows the security sensors to play a larger role in the intelligent home than just detecting intruders. Various sensors in the home, including motion, temperature and light, act as eyes and ears for the intelligent home. Some examples of intelligent integration of security with other systems include:

- When the security system is armed to holiday mode, lights and music can be switched on at suitable times in the day or night to give the impression that the house is occupied.
- Automatic garage doors and gates can be opened or closed with a single control that arms and disarms the security system at the same time.
- The heating in the home can be automatically switched on or off or turned up or down in response to the security system being armed to away or night mode or by time programmes.
• Schedules or time programmes allow automatic control of security, lighting and other appliances. These can be used to automatically arm the security system and switch off selected lights at night, and, for example, to water the garden. Some advanced systems calculate the sunrise and sunset times based on the time of year and location which can be major cities in the world or latitude and longitude coordinates. Automatic adjustment of daylight savings time changes is also a very useful feature for time programmes as it removes the need to remember to change the time manually.

• Motion sensors in certain areas in the home can trigger the alarm in away mode, but can turn on certain lights in night mode, and switch them off automatically when no more motion is detected for a period of time.

• External motion sensors can switch on lights and trigger a recorded warning message.

Security and lighting
The most common component of a home automation system is lighting, where one or more lights can be controlled by electronic switches, keypads or remote controls. Such lighting systems may be bus based like KNX or C-Bus by Schneider where electronic low voltage switches are connected in a bus throughout the house, and the lighting loads are connected directly to relays or actuators rather than through electrical light switches.

Bus lighting systems are very reliable and have very extensive functionality. However, they will probably not be found in the average home due to the cost and the fact that some electricians are not yet familiar with the wiring scheme. When such bus systems are installed in a home, KNX or C-Bus enabled security systems which work directly with the lighting system are a great advantage as they allow the security system to directly control the lighting, and conversely allow buttons on the lighting system or touch screens to operate the security system. Lights and appliances can also be connected via the AC outlets using power line technology like X10 and its variants, although this is more suitable for non-essential items like plug-in devices because of problems caused by noise on the power line.

Other lighting products communicate by wireless means like infrared and RF signals. Wireless technologies used in home automation, including products complying to the Zigbee and Zwave standards, are expected to be more widely available at a lower cost in the near future. Sound and entertainment multi-room systems controlled by touch screens and keypads that also control lighting with mood scenes and under floor heating are a typical part of home automation for high-end homes. The cost of such systems ranges from many tens-of-thousands of Rands, to more than six figures but these are not an essential aspect of a home automation system.

Practical
In summary, home automation is not just for the very rich, with full scene control of every lighting circuit, and entertainment systems with touch screens in every room. It should be understood that it is not necessary to be able to control every light and appliance in the house, to have a practical home automation system. Any reasonably sized house can be a candidate for automation. The key to practical and affordable automation is the integration of strategic appliances, security, lights, and other subsystems in the home to create an intelligent home which provides comfort, convenience and energy savings for the occupants. There is a large untapped opportunity to bring affordable home automation incorporating smart security systems to a much wider market.

HomeIQ is the sole distributor of the Comfort Home Automation Controller in South Africa and can be contacted at info@homeiq.co.za
The big five in estate security

By Andrew Page Wood, VideoIQ Africa.

Effective security in South Africa remains a challenge. Unlike many western countries, we are faced with circumstances and realities here that make protecting people and properties unique. As a nation we rely heavily on guards and conventional CCTV systems to protect us. This has been the case for years, but our notorious crime statistics are testament to the fact that this is failing.

Now, overlay this with the fact that we have more walled developments and especially golf courses than most countries, which over the last 20 years developers have fenced in and built into lifestyle estates.

The result is a R50 billion a year industry, with us ranking as one of the very top spenders in the world with a staggering 806 security personnel per 100 000 population... and crime keeps increasing.

Talking of estates now, in my experience they typically use the same three elements for security and have been employing this strategy for years:

- Perimeter security fencing (some with zone alarms).
- CCTV camera systems (many with motion detection).
- Physical guarding services.

These often work in combination and have fundamental weaknesses that we will explore. Some estates have historically spent enormous amounts of money on security and CCTV systems but have neither been able to crack down on incidents nor see any return on investment to measure their success.

Residents and homeowners associations (HOAs) are now fed up and are starting to ask hard questions about where their spend has gone.

The big five

1. Reliance on guards. Guards have two jobs to do. The first is observational, observe and report. The second is much more adrenaline pounding, fight or flight, respond, react, chase, apprehend. It’s a lot like being an anaesthetist, 99% of the time work is the same old boring routine, but the last 1% is terrifying. Sadly, our brains are not designed to do the first part, the non-stimulating routine stuff, so we slip into what is called Theta frequency or meditative day dreaming. It’s completely normal.

2. Beams, walls and fences (with zoning). It’s astounding how much estates can spend on this. Walls get higher, fences get doubled and budgets go up. Here I see the problem as follows: the fence/wall in itself now becomes a barrier that needs to be armed because it cuts visibility and needs to be protected as an asset itself. Security staff often rule out threats, underestimating the odds of penetration.

Further, often sections are zoned or have beams, alerting the control room when triggered. This is crazy. Guards rush to a zone that has gone into alarm with no information at all to use, it’s much like a beam or sensor going off at home...what was it, a dog, people, how many, going in or going out, or just a false alarm?

It’s critical that zones or beams can give information to the response guys to verify, and the proven way to do this is through video so that they know exactly what is happening and how to react. It’s very simple these days to connect fence inputs and beams to camera inputs that trigger the video at the same time, simple and worthwhile.

3. Streaming CCTV video cameras (with motion detection). I’ve seen it time and again, some poor operator sitting in a control room staring blankly at 120 (very impressive looking) camera images with a job description that gets him fired if someone gets past a camera and he doesn’t pick it up.

Now, add motion detection to this scenario. The HOA decides to spend budget to help detection by adding software that picks up information at home...what was it, a dog, people, how many, going in or going out, or just a false alarm?

It’s completely normal.

It does not work.

So, the expense and reliance on humans to constantly monitor and detect threats either by watching a screen or patrolling a fence is a big mistake. Even the military is automating its guarding these days.

The solution is to take that same budget and use it to implement an E-guarding system that detects incidents before they happen, a system that continuously observes and monitors 24/7 in all conditions, taking all the pressure off the guards. It’s proven itself over and over and makes complete financial sense. Now your guards have a real job to do, they’ll know exactly what to respond to and when.

By Andrew Page Wood, VideoIQ Africa.
The solution is proper video analytics. Make sure you can give each of your cameras a real job description. So many companies claim that they can do this and it’s a dangerous claim. It’s relatively simple to analyse video data from a CCTV camera, work out that something is moving and box it, but it creates havoc for controllers due to false alarms. This is where analytics is really put to the test, it should only report when an alarm is real. So make sure you know what you’re buying and get to see it working in all conditions first.

4. Complex networks = error prone systems. Running a network, whatever type it is, outdoors over a 7 km stretch that combines electric fences, zones, sensors, CCTV cameras, guard check systems, power sources and whatever else an estate may have chosen for security is a nightmare to install and maintain. There’s just too much that can go wrong, especially with an IP camera system (not to mention an HD camera system which quadruples the problem). You see, IP was not designed to carry video. It was designed to send spreadsheets at most. So, trying to stream 120 cameras from all over the place back to one point where one collects and processes video is not smart. If something goes wrong anywhere, it’s going to quickly bring the system down. Also, video is going to be affected by anything that happens between the camera and the server (the head end).

Sadly many estates that have decided to invest in great technology have spent as much on their infrastructure and backbone as they have on the system. It does not need to be this way. The solution is smart camera systems with internal storage that process video at the pole. By moving as much processing and storage as possible away from the head end to the camera makes it 90% lighter on the network and dramatically reduces network traffic, bandwidth requirements and overall infrastructure costs. Best of all, even if your network is down your cameras aren’t.

5. Total cost of entry and ownership. If you add up all the budgets associated with the four points above you’ll quickly find that many estates have been burned and have spent vast amounts on fences, systems and networks that have not solved their problem. So many technologies and suppliers have over promised and under delivered, leaving a bad taste in the mouths of homeowners. Bad news gets around fast and sometimes this can affect not just the morale of the community, but can also impact on the market value of properties in the estate.

The solution is that HOAs and estate managers should not believe that they cannot afford the best technology. It’s time to think differently about this challenge and shift our approach completely. It’s simple. Take the overall annual spend on guarding as well as the budget for technology and roll them into one. Then, with a clean sheet, re-allocate and you’ll find that it all adds up fine. In fact, I’ll bet that there are probably some significant savings with a better solution overall.

So, speak to other estates that have been successful and find out how they’ve done it. Ask to visit sites and see for yourself what can be done. Don’t overspend on stuff that is not core to a solution, like expensive robust networks or software that has not proven itself. Finally, don’t buy until you’ve seen a solution working on your site at 3am in pouring rain on a windy night. Then you’ll know you’re covered.

For more information contact VideoIQ Africa, 0861 VIDEOIQ, info@videoiq.co.za, www.videoiq.co.za
Security and convenience by SMS

The TX-SMS unit is the ultimate in home automation security and convenience. Designed to empower end users in multiple ways, it can send messages as well as execute functions such as activating and deactivating alarms, switching lights and irrigation systems on and off and even monitor electric fences. It can also unlock gates and doors by SMS or a missed call in order to grant reaction officers or visitors remote access, hence its growing following in residential complexes.

“With all the pressures of modern-day life, it’s inevitable that at some point or another, people are going to forget to turn on or off geysers, or arm or disarm their burglar alarms,” says Tinus Jansen van Vuuren, regional branch manager for Elvey Security Technologies. “That’s when a nifty product such as the TX-SMS will really make a difference, because all they need to do to rectify the situation is send an SMS.”

He explains: “The TX-SMS is an important security tool owing to its ability to send alarm and contact ID signals to cell phones, as well as arm and disarm alarm systems and switch on lights ahead of one’s arrival back home, in the dark.”

Aside from its security benefits, the TX-SMS also makes life a lot more convenient. “It will open the gate and garage door for you and switch on the lights ahead of you arriving home. It’s a brilliant guest management system for B’n Bs and hotels, and it’s a lifesaver for out-of-town home owners who need to be able to give their family or staff members access to their properties,” says Van Vuuren.

Popular among security system installers throughout the country, the TX-SMS represents telemetry/alarm monitoring and remote activation technology at its best. Which is why it’s being increasingly deployed not only in the residential and hospitality sectors but also in the agricultural and industrial industries. “Farmers use it for controlling their irrigation systems and pumps remotely as well as opening gates. Industrialists favour the technology owing to its ability to monitor and report on applications such as tank levels.”

The TX-SMS is equipped with four hardwired inputs and two onboard relays which can be controlled remotely (switch on, switch off, pulse or toggle) by SMS, missed call or timer. Two of the inputs are optical isolated to accommodate the demands of industrial and high voltage applications such as electric fences and mains monitoring. To this end, the system boasts analogue and AC inputs for mains fail/restore and low battery reporting, notes Van Vuuren. It also boasts a tamper vibration sensor.

The unit is able to send SMSes to up to four reporting numbers while up to 500 different cell numbers can be programmed to control the relays by missed call. End users can programme it to SMS reports to them confirming and recording phone numbers as well as actions executed. They can also set special access rules limiting the relay control to a certain number of calls per time window and on specific days of the week.

User definable SMSes or Contact ID allow for monitoring and reporting on the state of inputs, he points out further, while its missed call functionality ensures cost-free opening of gates and doors.

For more information contact Elvey Security Technologies,
+27 (0)11 401 6700, tasha.smith@elvey.co.za, www.elvey.co.za

Easy, yet secure access

Security in complexes and estates is a high priority.

Security in complexes and multi-dwelling establishments is a high priority issue in the minds of discerning owners and residents. The most visible and regularly utilised aspect, for residents and visitors alike is, of course, access control on entry/exit.

How often have you found yourself, as a resident or visitor at the entrance/exit of a complex or multi-dwelling establishment, tapping your fingers in impatience on the steering wheel as motorists ahead of you wrestle with a cumbersome and grubby old book or clipboard? Each driver fills in copious details in blocks that are never big enough, wondering, as they do, if anyone will ever look at or check up on what has been written, as they laboriously sign in or out.

Comb Communications has recognised the need for speed and efficiency at entry/exit points. Our people-focused technology has transformed the tapping of fingers on steering wheels into the quick tapping in of a simple code, into a keypad linked to our online system, the MK II, with far-reaching reporting capabilities.

This user-friendly add-on offering to Combi’s MK II access control system aptly bears the name TAP TAP (Temporary Access Pin). The first GSM intercom system prototype was installed in 2004 and is still up and running. Residents simply send a message to the application, which in turn sends back, via SMS, a unique, computer generated code which is then forwarded to prospective visitors for use at the gate. Comb recognises the need for gate personnel to be familiar with the correct use of the MK II system and the TAP TAP add-on. Training is given to guarding companies in this regard. Similarly, installers are trained to ensure that both the MK II system and TAP TAP entrance/exit keypads are expertly installed.

Comb has collaborated with Centurion Systems, Vodacom and Nashua Mobile, and MK II and TAP TAP users benefit directly from the alignment with these providers.

For more information contact Keep Access Control Systems,
+27(0)11 805 0175, siska@keepacs.co.za, www.keepacs.co.za
Surveillance on par

Bidvest Magnum Technology and Cathexis analytics solves perimeter intrusion at Prince's Grant Golf Estate.

Prince's Grant Golf Estate is on the Dolphin Coast of KwaZulu-Natal. This golf estate has recently upgraded its security system including its CCTV infrastructure.

Prince's Grant required a system integrator to implement a turnkey integrated security solution that would cater for access control, CCTV, electric fence, biometrics and physical security. Bidvest Magnum came up with this solution that catered for all these needs in a phased approach.

The first phase was the installation of a multi-core single mode fibre backbone, which was installed around the 5 km perimeter. This fibre backbone is core to the infrastructure and has CCTV, access control, IT services and the electric fence alarms branching off it.

The cameras were installed around the perimeter electric fence line and are strategically placed so as to detect and alert the control room of any perimeter breaches. The intelligent video analytics of the Cathexis DVR successfully detects any perimeter breaches. When someone is detected, the control room is alerted with an alarm and the video of that specific camera pops up on the video wall, alerting the guards of the breach.

**Control room**

The control room is monitored 24/7. The cameras used are the Seawolf with an integrated housing with twin IR (100 m), 5.0-50 mm varifocal lens, 690HTVL effective, which picks up any movements day or night.

The control room has been secured and ergonomically fitted out with a video wall that houses 3 x 32-inch LED screens and 2 x 42-inch LED screens. There are two 42U cabinets, that house the DVRs in the one cabinet and the other has the fibre infrastructure kit. The security guards sit comfortably and view the 104 cameras on these screens and control the video from there. The Cathexis Cat Vision DVR provides full control over surveillance video playback, making it easy for the security offices to quickly retrieve evidence and speed up response times.

The three beach turnstiles have Axis dome IP cameras and the control room has bi-directional audio through the CCTV system to these turnstiles, to talk to and assist guests and homeowners at these points.

The major functionality of the Cathexis system is:

- Interactive maps with the capability to drag and drop cameras from the map interface into the viewing monitors.
- The ability to move PTZ cameras from graphic representations of pre-set positions on the map.
- The CatVision Tracker algorithm which automatically moves PTZ cameras to follow objects around the perimeter areas.
- A virtual matrix with auto-switching of selected cameras to selected monitors upon motion detection events.
- Bi-directional audio functionality using Axis camera audio capability and controlled via the CatVision user interface.
- Future functionality is to include integration with other third-party systems.

**Cathexis benefits**

The Cathexis health monitoring feature enables both on-site and remote analysis of the system and provides automated system failure analysis and prediction. And with Cathexis products being 100% South African and developed in KwaZulu-Natal, this ensures excellent support.

“The proven track record of Bidvest Magnum's installations, project management and regional structures combined with Cathexis system sustainability and backward compatibility along with the relationship with Bidvest ensures that Prince's Grant will have a sustainable security solution for many years to come,” says Kevin Monk, technical director of Bidvest Magnum.

Chris Van der Merwe, the CEO of the estate is confident of his security choices which secure the properties and homeowners and visitors of Prince’s Grant. “We were impressed with the professional manner in which the project was handled, and the quality of the installation delivered by Bidvest.

“The surveillance system has played a critical role in helping Prince’s Grant ensure public safety and protect its homeowners and visitors from damage and theft, and also allowed us to utilise our manpower on site more effectively. The system delivers a lower total cost of ownership because it provides greater image quality and reliability, and requires less maintenance.”

For more information contact Cathexis Africa, +27 (0)31 240 0800, gusb@cat.co.za, www.cathexis.co.za
Camsecure, a projects-based security solutions company, has incorporated a comprehensive surveillance system at the picturesque La Petite Provence residential wine estate in Franschhoek, Western Cape province.

In spite of the fact that crime statistics for this upmarket estate remain fairly low, the residents felt that the previous, outdated CCTV and access tag system needed to keep pace with new technology and trends. The estate is situated on a 36-hectare farm so the area of coverage is fairly large.

Camsecure’s MD, Francois Malan, pointed out that the residents had expressed the need for a system that would allow easy access, while providing security controls. “The administration of the existing access control card system was cumbersome and problematic.”

Phase 1 of the project was awarded to Camsecure in March 2012. The proposed solution was based around the Milestone licence plate recognition (LPR) software and included Axis cameras. “The critical point for Camsecure was ensuring that all systems could be readily integrated. Single-vendor solutions, without the ability to integrate with other third-party hardware and software are not cost-effective or sustainable,” Malan explains.

Axis and Milestone

“The Axis network camera, fitted with an infrared illuminator, offers superb video performance and provides images with better contrast, clarity and resolution. Milestone’s LPR software allows registered vehicles to access the estate easily, thus eliminating any possible traffic jams at the entrance. We also have the ability to institute a dual system using both LPR and access cards if required,” Vivian de Meillon, regional manager for Camsecure Cape Town adds.

“The LPR software accesses a database of all resident vehicle number plates and thereby issues an instruction to the access boom to be raised when a valid number plate is registered,” he added. The surveillance solution makes it possible to blacklist vehicles that have been red-flagged for any reason.

“The second phase includes the monitoring of the estate’s perimeter,” says Malan.

The roadside perimeter will be monitored by surveillance cameras, networked with the entrance camera on Milestone’s software. There are a number of streetlights at intervals along this perimeter which provide a degree of ambient lighting at night. “We debated whether to use thermal or low-light cameras for this installation, but since the main intention is to alert the security guards to any intrusion, we felt that the Axis Lightfinder technology camera was the ideal solution,” Malan explains.

Seeing the light

The Lightfinder technology incorporates a CMOS sensor with exceptional light sensitivity. The advantages of the Lightfinder technology are high light sensitivity, excellent image quality with low noise but a wealth of details, and better colour reproduction in low light.

In order to reduce the carbon footprint of the installation, Camsecure elected to deploy wireless, solar powered technology in place of copper cables powered by electricity. “Not only is the use of wireless, solar-powered communication environmentally friendly, it is also very cost effective and flexible in terms of current and future installations. No excavation for cable routes is required and additions or changes to the current system can be readily and quickly implemented,” says Malan.

The phase 2 installation will include video analytics that will inform the security guards of event-driven incidents when a breach of the perimeter is detected. “When an alarm is activated, whether by the entrance camera or a perimeter camera, the guard will receive notification on a monitor of the mapped incident area as well as the video feed of the incident. By locating the camera responsible for activating the alarm, he will be able to accurately pinpoint the area of concern and react accordingly. The system can also be programmed to provide the security officer with instructions. This provides a complete audit trail for each event,” notes Malan.

For more information contact Camsecure, +27 (0)11 781 1341, francois@camsecure.co.za, www.camsecure.co.za
Condomínio Vila Fontana in the city of Maringá in Brazil is a gated community that from the start sought to provide the most complete security possible for its residents. To that end, it sought a solution that combined video surveillance with license plate recognition (LPR) and facial recognition tied into its access control system. They not only wanted to be able to recognize the license plates of those entering and exiting the residence, they wanted faces associated with those plates. In that way, they could be sure that no one was entering under false pretenses and with possible criminal intent.

Their research of vendors led them to Intelligent Security Systems (ISS), which was recently voted the leading vendor of Video Management Systems (VMS) in Latin America by IMS Research. ISS has had experience with such applications, and in addition to its SecurOS VMS solutions, has analytics such as LPR and facial recognition built into the software as well. It was also known that ISS was involved in providing security solutions for the Presidential Palace in Brazil.

The installation
The integrator in this case was Speed Sistemas and it involved nine Sony IP cameras. There are five cameras equipped with SecurOS Facial Capture and Recognition systems and a 500-face database, along with a SecurOS LPR system.

The cameras were placed at the gated entrance and in order to gain entry both the license plate and face of the driver must correctly match the information in the system. Because of the high profile nature of some of the individuals who live in this community, nothing can be taken for granted in terms of security. The access control system at the gate does not let a vehicle through unless it clears the security procedure.

Both residents and management are very satisfied with the current system as it provides additional layers of security that assure that those entering and exiting the residence are properly vetted by the system. In this case, this is something that is done in an automated fashion, which saves the time and expense of security staff having to check every car and driver.

This has made this residence all the more appealing to others, who have learned of its reputation for top security that employs the latest in security technology. Condomínio Vila Fontana, which was already known for its very appealing layout and location, has grown even more in popularity because of its reputation for also being very secure.

For more information contact ISS South Africa, +27 (0)83 330 8767, Eugene.Kayat@isscctv.com
Back to school
By Allyson Koekhoven.

Integrated solutions are key to security in education.

Hi-Tech Security Solutions went back to school to learn about best practice solutions for security installations at educational institutions. According to Walter Rautenbach, MD of neaMetrics, the landscape of educational security installations has changed from just addressing general risk issues to the need for a totally integrated solution for campus environments.

“Some of the needs that these institutions, specifically with regard to tertiary education, try to address include the general safety of students and staff as well as the security of assets, on campus/premises. This involves controlling the people entering the premises who actually have a right to be there and who have paid their tuition. It also looks at how they can secure equipment in laboratories; control how long students spend in labs for practical exams, and general control of student attendance,” Rautenbach explained.

“In primary and secondary education, parents are starting to consider such solutions for attendance purposes. This is not necessarily just to make sure that their children attend school, but also to have some form of early detection should their child not actually show up in the classroom. This latter point has become an increasing concern as the fear of child abduction continues to be headline news,” added Rautenbach.

John Powell, MD of PowellTronics, agreed and added that an increasing emphasis on occupational health and safety (OHS) compliance is a large issue of concern. “Typically in the past, educational facilities maintained an open door policy, but with both the increase in crime, as well as the sheer magnitude of people entering the facilities, more attention is being paid to controlling the flow of people.

“Together with the high volumes of traffic in educational facilities, other challenges are presented in the large geographic size of the facilities, the often widespread campuses and the classification of older facilities as heritage sites. This latter point means that it is often difficult to deploy technology because of the restrictions placed on any form of architectural alteration on these buildings.”

Allied to the large volume of people entering the premises is the huge number of entries into the access control database. It is not uncommon to have 20 000 to 40 000 people on a tertiary education campus database. If one then multiplies this number by more than 500 different access points, it clearly becomes a management nightmare.

“A common complaint we receive is that the service provider has installed a database that cannot cope with the sheer size of the institutions database. Another key element is ensuring that institutions chose a database that allows seamless integration between the access control database and the institutions’ ERP packages, like SAP, and Microsoft Active Directory,” Powell added.

Ensuring that the person writing an exam is the person who registered for the course is another priority for tertiary educational facilities. “In addition, the educational institutions have extensive computer labs and they need to monitor time allocations in terms of IT usage and protection of these high-value assets. Another issue cited by educational institutions, is the management of vehicles in terms of where and for how long they may park.”

Powell said that CCTV surveillance is often utilised as a deterrent measure. “Access control is a more pressing concern, but it may be integrated/linked to the CCTV cameras in areas deemed to be sensitive, this will allow access control transactions to be coupled with CCTV footage. Biometric access control is beginning to gain popularity for entry into these sensitive niche areas. However, for now, student cards will continue to be the access method of choice. Hybrid installations, combining both technologies, are becoming more common at most educational facilities.

“By linking the student card to access control software, one is able to ensure that students are permitted to enter only predetermined zones. From a physical perspective, it is often difficult to deploy turnstiles due to space constraints and possible bottlenecks due to the vast number of users, but these are considered appropriate for student entry into hostels. Controlling access to hostels is sometimes a challenging task, as often these facilities are used by non residents for functions and eating halls, however if enough prior investigation with the various role players is done, there are viable solutions,” said Powell.

“In its simplest form, the student card is used for identification for third-party student discounts and access control. Some institutions take it a step further by indicating they want to extract value by implementing more intelligent card solutions. These would carry value that can be utilised on campus for purchasing of services such as making photocopies, vending machines or buying refreshments in the canteen. Others have expressed a wish to give students credits for good attendance,” added Rautenbach.

The issue of database management can be resolved by screening potential service providers to ensure that they have experience in this arena. Typically, a service provider should be utilising the latest IP technology and non-proprietary databases. It is hugely beneficial if the system includes a self-monitoring and early warning system that sends alerts to relevant parties when the database or communication to the systems controllers is becoming too large for sustainability. Finally, the system should be able to accommodate numerous shift parameters and offer flexible access groups,” said Powell.

Tomorrow, tomorrow
Rautenbach said that the spotlight will remain on the total offering provided. “We feel that the focus on fully integrated solutions that address the end user’s needs will increase and more market consolidation will occur. When we say ‘integrated solutions’ we are referring to end-to-end solutions; solutions that integrate various aspects of security including access control, CCTV, workforce management, time and attendance (T&A) as well as more sophisticated building management solutions, with a focus on green, environmentally-friendly implementations. “The client should not be expected to seek out a company that can integrate all elements of the total solution. Service providers need to become more proactive in forming symbiotic, collaborative relationships with other service providers. In this way, the client will receive a completed, multi-modal system that addresses all their specific requirements,” Rautenbach concluded.

By Allyson Koekhoven.
Solutions for Education Establishments
High quality solutions backed by world-class reliability and customer service.

Keeping the learning environment safe. Bosch is committed to developing and delivering advanced technology security solutions that meet the needs of 21st century buildings and lifestyles. One of the most important areas where this commitment to delivering only the highest levels of security plays a part is in schools, where the safety of both children and staff members are paramount. Visit our website at www.boschsecurity.co.za or contact us on 011 651 9600.
While South Africa hasn't had the mass murders that some educational campuses in the USA have experienced, our local campuses are by no means a beacon of security for staff and students. Crimes which occur far too often (those that are openly reported) include rape, theft, vandalism, intimidation and the usual assortment of South African crimes. Given that our universities are a hotbed of political activism and, in some cases, freedom of speech and thought, demonstrations and the violence associated with them are also a factor to consider in campus security.

The Campus Protection Society of South Africa (Camprosa) held its annual conference at Sun City late last year to discuss the various issues universities are facing and included presentations on security as well as other pertinent campus topics. Hi-Tech Security Solutions was able to attend some of the presentations and found that South Africa's campuses face similar problems to those in other countries, the difference is in how these issues are dealt with.

After an opening address by the president of Camprosa, Roland September, the keynote on the first day was presented by Anne Glavin, director of police services, California State University and president of IACLEA, the International Association of Campus Law Enforcement Administrators (www.iaclea.org) and Ray Wheatley, IACLEA international regional director from Dublin City University. IACLEA is an organisation focused on advancing the skills and knowledge, as well as promoting effective campus security internationally. Glavin added that it also strives to enhance the image of the campus security professional while ensuring proper governance of these operations. IACLEA has embarked on expanding the training facilities available to members using the Internet, through mediums such as webinars, and it is also building a campus security portal to facilitate communications and education among professionals across the globe.

To date, IACLEA has 1 195 members in 20 countries and is looking to expand its international membership to facilitate more information sharing and effective communications.

Information is vital
Jenny Reid from iFacts was up next, speaking about screening employees. She notes that while companies often screen top employees, they fail to validate contractors and outsourced staff, of which campuses use a substantial amount. In addition, when checks are carried out, they focus mainly on criminal records and not on credit reports, the validity of the person's ID, driver's licence or educational qualifications etc.

Reid advocates the use of a single database for the security industry where employees' employment history is held. This could be used to validate people's identities and prevent syndicates from sending the same person to various security companies to commit fraud.
The section commander of major events at SAPS took the stage to discuss the safety and security processes involved in holding large events. For events that will have more than 2 000 people attending, the organisers need to ask for permission for the event and have an emergency plan in place.

This does not mean smaller events can get away with no emergency or evacuation plan. Even low-risk events need a safety officer and to ensure they have reasonable measures in place to deal with an emergency. For larger, annual events, plans must be submitted to the national commissioner six months in advance and contain sufficient details for it to receive a risk classification. He notes it is always worthwhile giving the national commissioner’s office sufficient time to work through the information and deliver a risk classification.

Sustainable education
Prof Johan Nel, executive manager at the Centre for Environmental Management at North West University spoke on the task of making campuses more sustainable. Sustainability is not simply a ‘green’ issue, but a project to enhance the environment in order to provide for today’s needs while ensuring that the people of tomorrow can provide for theirs.

Nel says sustainability is a journey, not a once-off project and this journey needs to include four elements: environmental performance, social investment, sound finances and good governance. There is no silver bullet in sustainability, but it needs to be an ongoing project that is continually advancing in small manageable steps.

Nel suggests legal compliance and compliance management is the first step to take, followed by efforts to reduce the campus’s footprint on the environment in small, incremental steps – aiming for low-hanging fruit to gain results and commitment. This includes improved energy efficiency, improved water consumption, waste management and enhancing biodiversity programmes and so forth. The first step for any university, however, is to get its own house in order first.

Marius Coetzee, MD of Ideco Biometric Security Solutions was up next, discussing the benefits of biometrics, specifically fingerprint biometrics as a means to positively identify people, whether for access control or transactional purposes. He also mentioned the ability to combine smart card and biometric identification in sensitive areas to ensure people who have access to bank details, for example, are accurately identified when going about their jobs.

The future
Dr Theuns Eloff, vice chancellor, North West University closed the final day’s presentations with a talk on what the future holds for South African universities.

Eloff started out showing how higher education played a vital and measurable role in economic growth as well as in the building of social capital. Expanding this thought, he added that any university that is aware of its place in the market will be focused on governing and managing itself with the goal of continuously improving its effectiveness and efficiency so that it can enhance its competitiveness.

He also discussed the problem universities have to deal with in the financial realm, including the decreasing contribution of the state to higher education. Eloff also supports e-learning initiatives which place the student at the centre of the learning experience.

Another aspect of campus success he mentioned was the need to make universities part of meaningful partnerships in order to ensure they become more relevant and responsive. This will lead to a change from the traditional management style of universities to more professional, accountable management that is market driven, proactive and strategic, and has a portfolio of funding options that no longer rely only on the state.

The final presentation Hi-Tech Security Solutions attended was by Paul Ochieng, dean of students at Strathmore University in Kenya. Ochieng spoke about the security issues universities in Kenya faced, which are exacerbated by the fast growth in the number of universities that have been launched in the country (there are a total of 71, with the majority of these launched in the past 5 years).

While universities in Kenya were traditionally government funded, more people are ready to pay more for private higher learning opportunities because of quality issues. The campuses are also political hotbeds and demonstrations, often violent occur over a host of issues. The sheer number of students serves to exacerbate crime problems. Ochieng discussed the processes Strathmore has put in place to deal with these issues, which local universities can also learn from.

Other presenters at the conference included Dr Craig Donald, the late Terry Scallan and Dr John Tlabe. The Camprosa national AGM was also held.

Camprosa has announced that the 2013 event will be held from the 3rd to 6th November 2013 at the Boardwalk Hotel and Conference Centre in Port Elizabeth. More information is available at www.camprosa.co.za

Suprema’s extensive range of fingerprint, facial and card access terminals are easy-to-use and suited to many environments. With options available for indoor or outdoor applications, Suprema gives you the choice.

Securing Campus Assets
- Positive student identification for access and exams
- Student and lecturer attendance
- Recording practical lab time
- Preventing unauthorised access

Enquire today
BioStar SDK allows for seamless integration into new or current systems.
Security trends for 2013

By Andrew Seldon.

What better way to kick off the year than to look at what the industry expects to see happening in the coming 12 months? Hi-Tech Security Solutions asked a few people what they were expecting in 2013.

We break the answers down into categories below, looking at technology areas as well as security associations and system integrators. As always, we welcome any comments from our readers as to what you think will define the market in the coming year.

To make things a little more interesting, we asked our respondents to not only talk about their areas of specialist, but to offer one piece of advice they believe will be crucial to customers in the coming year.

CCTV, surveillance

Axis Communications
Roy Alves, country manager for Axis Communications says the surveillance market will see a continuation of what happened this year. He expects better WDR (wide dynamic range) and a focus on image quality in more complex lighting environments. “Another trend is low light providing colour information.” He adds that people are starting to ask about Ultra HD, x16 the resolution of 1080p (http://en.wikipedia.org/wiki/Ultra-high-definition_television). And he expects H.265 will be massive next year, assuming it does launch in 2013.

As far as buyers opting for one brand in their solutions or preferring devices from multiple vendors in a best-of-breed installation, Alves believes there will always be requirements for single branded solutions. “As Axis we will always want to offer that as a turnkey solution with one point of responsibility. However, looking ahead, third-party integration offers many advantages to the customer, allowing for best-of-breed manufactures on a single open platform.

When asked what one piece of advice he would offer customers, Alves says: “Select a focused vendor who has invested in their local regions (support, sales, RMAs and marketing). There is a lot to be said about international manufactures that have local offices in our region, it really is a long term relationship.”

Miro Distribution

Alex Bantjes, Miro’s brand manager for Vivotek believes 2013 will be a historic year for the surveillance industry, one in which we will see the tipping point in the IP vs. analogue debate.

“School’s out… IP is the way forward. This trend can be clearly seen throughout training sessions hosted by ourselves, there seems to be an ever-decreasing number of attendees that have not had some level of exposure or experience with IP surveillance products. I also believe that more IP professionals will be seen in our industry going forward.”

Miro’s MD, Bertus van Jaarsveld expects to see more high-resolution megapixel cameras being used as well as innovative camera formats such as the new fisheye cameras offering multiple views and post-event digital pan/tilt/zoom.

As to what technologies or technical implementations will stand out in the coming year, Bantjes expects new technologies such as scalable video codec (SVC) and video push technology, along with a drive towards edge-based mobile/independent recording solutions. “With new compression technologies such as SVC and increased SD card sizes, we can now get more data stored on edge than ever before.”

Van Jaarsveld says the market is finally starting to adopt wireless solutions for IP surveillance projects. “I believe we will see a marked increase in the number of large surveillance projects making use of fixed wireless networks as well as some interesting implementations with wireless mobility.”

As for good advice, Bantjes advises customers to do as much research as possible and thoroughly assess their demands.

Avigilon

Ryno van der Vyver, regional sales manager for Avigilon, Africa, also expects the “upgrade transition from analogue to high-definition surveillance systems will gain more momentum in 2013.” With high-definition multi-megapixel surveillance you can cover larger areas and get amazing image detail. The systems are affordable and it is becoming much easier to effectively manage millions of pixels contained in video footage through powerful, feature rich and intuitive software that can accommodate both analogue and multi-megapixel cameras.”

He also expects the image detail available in high-definition surveillance will result in new business intelligence applications for surveillance appearing in addition to the traditional security, safety and risk mitigation applications.

Van Der Vyver also believes security systems that will stand out in the coming year will pull ideas from the gaming industry to help with ease of use. “When users interact with systems and feel engaged instead of frustrated it creates efficiencies and a positive response. I also think that the security industry will embrace discussion and the exchange of information through social media as it makes it easier for customers to rate their options.”

Van Der Vyver’s advice to customers is: “before you spend money on a large security system, request and check up on reference site installations from system integrators and manufacturers. Sales people often display the logo of all the major brands during the presentation, but establishing if they really do have a satisfied customer or one that is even aware of their claims is key to avoiding purchaser’s remorse.”

Access control and identity management

neaMetrics

Walter Rautenbach, MD of neaMetrics says, “Listening and speaking to guest speaker John Shi from A&S at the Suprema Global Partner Program a week ago only reaffirmed what we talk about every day. Distribution
doesn't need to change, it is changing. Distributors not offering SI are dead in the water. “

The solutions and technologies that will make a difference this year will be those that save end-users money by optimising operations. “We have seen a massive interest and growth in our biometric workforce management solutions, particularly in large outsourced environments such as guarding and cleaning services. Employers on the one hand want to minimise overtime and remain profitable, while large property investment companies, specifically in the retail environment, want to ensure they get the services they pay for. Companies are coming to the realisation that the initial hurdles, such as capital expenditure, should not stand in the way of ongoing sustainability. Inevitably, those who can control cost will survive and those that defer the expense will find themselves losing business.”

Rautenbach supports the Software-as-a-Service (SaaS) concept that saves customers from forking out capital for software that no longer fulfils business requirements in a year’s time. “The SaaS approach, in conjunction with a licensed approach, allows us to offer our client more value. Offering hosting facilities and related services to our reseller network also puts more options in their hands to offer their end-users.”

As far as advice is concerned, Rautenbach says look at the total value of the solutions being presented. Also, always consider if the company you are deciding to buy from has the skills and capabilities to integrate and customise solutions to your requirements, and ensure that you and your suppliers’ definition of integration is the same.

HID Global

Robbie Truter, area sales manager for HID Global SA expects to see a converged credential in a single card, which could be an ID badge that enables the user to get into the building, log onto the network and gain secure access to the applications and other systems they need. They can also use the card to gain remote access to secure networks, replacing the need for a one-time password (OTP) token or key fob. “A converged credential is more convenient for users, negating the need to carry multiple devices or re-key one-time passwords. It also provides greatly improved security, by enabling strong authentication throughout the IT infrastructure on key systems and applications, rather than just at the perimeter.

“We also see the adoption of mobile access using NFC technology. This is the use of smart phones with NFC to open doors and other applications that would emulate the card environment, but with the convenience of a phone. People lose their cards and keys, but never leave their home without their phone.”

This requires rethinking the way physical access credentials are managed. Traditionally, the card and the credential have been inseparable. However, to accommodate the mobility of that credential, it must be decoupled from the container. In other words, it must be possible to manage the credential independently of the physical device on which it is stored. As a result, organisations needed to be able to manage their users’ access, and quickly add and remove users from the system, without having to physically control or touch the device.

What matters to customers, says Truter is that a holistic, coordinated approach makes sense, physical and virtual security have traditionally taken place in two different domains, with very little visibility into what the other is doing. The more these groups work together, the better they understand the role each plays and the better the overall access experience and security. Ultimately, the goal is to come together and deliver a single access solution, with strong authentication, that is convenient for end users and cost effective to deploy and manage.

Impro

Impro’s sales manager, Linda Glieman believes one of the biggest trends will be around ease of entry without compromising security, and more Web-based solutions. Also critical this year will be the ability to provide a product platform that has a strong integration ability to ensure that a company’s total security requirements are met. This extends to the ability for systems to integrate into a single monitoring platform/front-end which ties all aspects of access control together.

“The consistent adoption of the use of biometrics for access control will continue to stand out in 2013. As installers are gaining more experience in the field of networks, IP based solutions will become more demanding, eliminating the need for long cabling runs and reducing labour time to install.”

Glieman’s advice for 2013 is to carefully consider the installation best practice used by the installer. “Customers must ensure the installers are accredited to supply and install the required solution in order to gain the most effective ROI and ensure their ability to provide an excellent maintenance contract backed up by good local support and repair service from the manufacturer. Customers must also carefully consider what warranty is supplied locally by the manufacturer and the technical support infrastructure in place to support the solution.”
System integrators

Camsecure

Francois Malan, MD of Camsecure thinks open platforms are where it’s at in 2013. “Integration will be a trend for the next five years. Business intelligence, information, asset registers and the like are becoming big news in the market. I do not believe that true cloud-based solutions, but rather hybrid solutions, will be a trend. I also do not believe that high megapixel cameras will be as big news as expected.

“I anticipate that we will see more intelligence in cameras, whereby they will be making the decisions in real-time. People want pre-filtered data, not to have to screen hours of recorded footage. They need immediate processing via cell phone, tablet or laptop. Video processing and analytics with edge storage will also reduce the pre-supposed acceleration and popularity of cloud-based storage.”

Good advice for customers, according to Malan is “Don’t be bedazzled. Look at international standards and broadcast standards instead of only considering proprietary brands that do not match global trends. Do not buy into a closed solution. Adopt multiple innovations.”

Jasco Security Solutions

Marius Maré, CEO, Security Solutions, Jasco Industry Solutions says system integrators (SI) will face “more IT and network related challenges as we see a definite move towards IP-based integration. Customers are now opting for a more integrated system solution and not only for CCTV and access control solutions.”

He says the increases in the use of TCP/IP platforms (including wireless) are happening for the following reasons:

• Most buildings have an IP platform already and make use of a WAN.
• PoE – Power over Ethernet, doing away with more hardware.
• Maintenance more cost effective, and
• Fault finding faster and easier.

When looking at technologies that will stand out, Maré has four expectations:

• IP solutions will continue to grow in 2013.
• Bringing the security, BMS and energy management onto one platform and sharing data on the WAN or cloud technology.
• More integration will be seen of products into third-party solutions.
• We have experienced an increased demand for thermal detection and satellite detection systems.

Maré’s advice for users is to choose a supplier, consultant and SI that listen to your requirements and challenges.

UTM

Kelly McIntlock, CEO of UTM says the shift from analogue to IP is going to be the trend in 2013 along with more business for thermal camera vendors. He also expects edge-based storage, compression and very high megapixel cameras to capture the headlines.

Additionally, he believes the economy will play a major role in the decisions around OEM or multi-brand implementation decisions, “but we have seen a major shift to single brand solutions”.

McLintock advises customers making decisions around security to spend more and not to try to cut corners. “It may save money immediately, but in the mid to long term it will cost you.”

Fire and safety

UTC Fire & Security

A UTC Fire & Security spokesperson says that while the economy has not stabilised fully yet, there is the possibility of an increase in government projects, but there will be continued pressure on integrators to decrease prices to remain competitive. The knock-on effect of this is that companies may be forced to downsize and some may even close. Despite this, there remains a serious technical skills shortage in South Africa.

With the proliferation of smart phones and tablets there will be a big move towards mobile applications in 2013. This will cover all sectors including intrusion, CCTV, access control and fire detection.

The company advises customers to take a long-term view, even though it is often difficult. Customers should focus on investing in quality products that have been certified by recognised authorities. The total cost of ownership will in most cases benefit from a higher initial investment.

Alarm and intrusion

Elvey Security technologies

Ingo Mutinelli, sales manager at Elvey sees some significant changes in this market. For one he sees more acceptance of wireless solutions as the technology has proven its stability and has a full feature set.

Visual verification through intruder products is another key area for Mutinelli. He expects to see many more panels offering visuals to accompany an alarm to allow the homeowner or response company to first identify the problem before dispatching a guard. This market will grow along with the increased use of the cloud, allowing home or business owners to receive real-time images of their premises via their tablets or cell phones.

As far as integration is concerned, Mutinelli says we are already seeing many previously independent security functions coming together. This includes video verification, as mentioned, but also other features such as alarm outputs on DVRs and so forth. He says customers want a single solution that does everything from one vendor. That way there can be no question of who gets the call when something goes wrong.

His advice for customers is to stick with reputable distributors and brands, there is a reason they have been around for so long. The bottom line is, “you get what you pay for”.

Tyco Security Products

Ernest Mallett, regional sales manager, sub-Saharan Africa for Tyco Security Products says a big influence in this space for next year will continue to be wireless alarms/ intrusion systems as additional functionalities are added and the underlying technologies continually improve.

“With residential wireless, new introductions will continue to satisfy consumers’ growing desire for mobile accessibility to all the systems in their home. For example, bi-directional wireless technology allows consumers to be able to access their residential alarm panel from anywhere – their office computer or smart phone. Video verification will be the next evolution in this area.

“The commercial side of wireless intrusion is really coming into its own thanks to improved battery life, reliability and security of the system itself,” Mallet says. “Today’s systems have 128-bit AES encryption to prevent the wireless signal from being sniffed or hacked, so the signal cannot be overtaken through the air. New commercial systems also have increased range for longer distances between panel and sensor without the use of repeaters and better noise immunity from interference from other appliances or systems.”

IP communications & network technology

Duxbury Networking

Andy Robb, chief technology officer at Duxbury Networking says
virtualisation is and will continue to be the biggest technology influencer in 2013. "That said, virtualisation will evolve from what we have seen up to now, which has been data centre focused, to more innovative applications of virtualisation.

"Virtualisation of the desktop, for instance, will be used to increase productivity and bring down costs. Virtualisation technologies will also be applied in the video surveillance and security arena, with new apps being made available to allow, for example, the immediate capture and playback of video footage on handheld devices including smart phones and tablets." He adds that the most important technologies of 2013 will be those designed to make our every-day lives easier.

“We can also expect a proliferation of green technologies and the use of electronic devices to monitor, model and conserve the natural environment and resources. New technical implementations will be used to underpin sustainable energy generation technologies such as photovoltaic, wind turbines and bioreactors for natural gas production.”

Robb’s advice to customers is, “ensure that your computing requirements have been correctly specified by an appropriately qualified and experienced consultant and match them to a solution that is best suited to your application, now and in the future. Don’t allow yourself to fall victim to an enthusiastic sales pitch that is without substance and foresight.”

Associations
ESIA
Anthony Rosenbaum, director of XtraVision and chairman of ESIA sees change happening for the security industry in 2013. “With the draft Amendment Bill about to be promulgated, I believe that the electronic industry is going to have to change, whether we like it or not. At present the electronic security industry is as fragmented as it has been for the past several years. With new legislation and perhaps a more concerted effort by the regulatory authority to control the industry, companies and individuals will have to start thinking seriously about becoming part of the industry.

Therefore, as the Electronic Security Industry Alliance (ESIA), which falls directly under the Security Industry Alliance (SIA), which already has a sound working relationship with government, a move to ESIA by the general electronic industry would give more credence to these companies and individuals in terms of becoming fully fledged members of the electronic security industry,” says Rosenbaum.

“Government will certainly become more involved in the electronic security industry over the course of 2013 and into the future. However, it is still premature to assume that their involvement will be in a positive way, as much as we would like it to be,” he continues.

“I would like to see far more co-operation between the various security associations; however, until personal agendas and other issues between individuals are ironed out, co-operation is going to be a hard nut to crack. I do, however, remain cautiously optimistic because when government and the regulatory authority start applying pressure, there will not be too many places to run to.”

SASA
Jenny Reid, MD of iFacts and president of SASA has a similar view on the Amendment Bill, noting that it is a serious concern for business. Most people in the industry thought it had been sent back for more work, but it is actually under consideration. The question of foreign ownership is confusing since most of the large guarding companies have some foreign ownership and there is no clear reason for the sudden turn against them.

Reid says PSIRA, the minister and industry need to work together to make the private security industry work. Arguing won’t reduce South Africa’s high crime rate or create a better life for everybody.

SASA is determined to work more closely with PSIRA to find ways of more effectively dealing with non-compliant and unregistered companies. Reid says the move to compliance must come from within the industry as well as from consumers of security services who need to be educated as to the benefits of only hiring compliant suppliers.

Once again, Reid agrees with Rosenbaum in that the industry has personality clashes which often prevents it acting in concert. However, she says SASA is focused on supporting any company that is compliant with PSIRA regulations.

Information security
Holton and Associates
When it comes to trends in the information security market, Jonathan Holton of Holton and Associates, Bitdefender distributors, says the talking point will be using the cloud for antivirus, especially for the smaller SME customers. Cloud systems will perform the same functions as the traditional server/client security system. A benefit of this is that the installation and setup of cloud solutions can be done by lesser-qualified technicians, especially because SQL database systems are not required. The jury is out on Windows 8 and Holton expects more installations on Android for Bitdefender.

For users looking at information security solutions, Holton advises to trial the top-rated products by AV-Test.org. "There are too many viruses hiding on data that is supposed to be protected and other antivirus systems can easily be checked to see if viruses have leaked through. One does not easily achieve the top spot without vigorous testing."

Magix Security
Hedley Hurwitz, MD, Magix Security sees the biggest trend coming from online apps. "We are very rapidly moving away from installing anything on our workstations because it’s a pain to have our functionality and data tied to a physical location, and because it’s a pain and endless costs for corporations trying to administer and secure what sits on our workstations. And if you securely store your data in the cloud, you never have to worry about backups or rebuilding your workstation after a crash. More applications will be ported to the cloud to take advantage of these new technologies.”

Cloud and mobility will keep growing and eating up traditional revenue streams and all related security solutions and systems will become even more critical to business risk management in the coming year.

"Making sure you, or your employee, is the only one who can access approved content, puts more burden and emphasis on the authentication process. First there is a growing need to secure device access. Once the device is authenticated, we need to confirm the identity of the user. I believe the adoption of biometric identity management is set to grow rapidly because, at the moment, we don’t authenticate, we approximate. Whether we use passwords, PIN codes or two-factor authentication, all of these only assist in approximating identity, not authenticating. Biometrics is the only reliable and viable option.

Hurwitz’s advice for 2013 is a recommendation that customers don’t make big capital investments in hardware or software. “Technology is moving too fast for any of us to predict the value of an asset a year ahead. Rather find the products and services that let you pay, and measure value, as you go. Obviously, whatever path you choose you have to ensure that you invest in the most appropriate security solution. It’s time that companies invested in a security environment that meets their risk profile and is not based on an IT budget.”
Specifying and selecting video surveillance systems

By Katharina Geutebrück.

In this article, the first of five, Katharina Geutebrück provides information and guidance to steer you through the important process of assessing your needs and defining your requirements.

This guide focuses on the video surveillance systems which are used for protecting buildings, sites and people and which may also be referred to as video monitoring systems, CCTV (closed-circuit television) or video security systems. Those designed for traffic monitoring, investigative surveillance or the quality monitoring of industrial processes known as machine vision are significantly different and fall outside the scope of this guide.

A video surveillance system generally consists of many different components. The illustration below shows the logical components, all or most of which can be included in a system. Since the advancing digitalisation and the increased use of high performance processors together with software or firmware components have produced enormous increases in both the flexibility within systems, and the performance capability of individual components, there are now often several logical components combined within an individual device.

For example we find compact cameras in weather-proof housings with built-in LED lighting; video analysis or storage functions in network cameras; video analysis options in recording devices; picture display and operation offered as a software package on a computer etc. The Technical Essentials section of this paper describes the technicalities of individual components and systems in more detail.

Good preparation and planning is vital

It is vital that each component is selected to meet the particular requirements of the application, and to be compatible with all the other components. Since the multiplicity available in the market seems endless and is difficult for the user to survey, good preparation and planning is all the more important. Only with good preparation and planning can the real requirements be formulated and suitable quotations invited. Let’s look at each planning stage separately.

Determining the aims

It is usual for a comprehensive security concept to already exist and for it to include the organisation’s protection targets, before the issue of video security ever arises. So the aims of the video security system can usually be drawn from this.

The most important question of all is: what do we need which information for, and when? Essentially, a video surveillance system does not supply anything other than picture information, so you need to answer this question as precisely as possible. Installing a camera first and then considering who should look at which pictures, is certainly not to be recommended as it usually leads to excessive costs and fewer benefits.

The majority of pictures generated by video cameras are totally irrelevant for the user and are never viewed. The key advantage of a modern video surveillance system is that it reliably provides picture information which is relevant, quickly and easily accessed, or better still switched to the screen when required.

The more precisely you can formulate your requirements, the greater the benefits the system will deliver. As is so often true, as far as pictures go, less is more!

Analysing the basic conditions

Most video surveillance systems are not planned and built on a greenfield site. There are often basic conditions which have to be considered, for example:

- Existing video components which are to be used again, such as existing cameras.
- Existing or planned third-party security systems to which interfaces need to be provided, for example access control or fence detection systems.
- Existing legal regulations which have to be observed, such as the German BGV C9 Kassen regulations.
- Legal limitations on the use of the system, such as data protection rules.
- Legal requirements for approval of the system, e.g. legal frameworks for worker participation and consultation.
- General and application-specific regulations and standards.
- The organisation surrounding the use of the system: issues such as whether you will use your own staff or a contractor, switch to a internal centre or external control centre at particular times of day, whether the police or others will also evaluate images etc.
- The time period within which a critical event should be, or can be, evaluated.
- These general conditions may give rise to limitations or to additional technical requirements for the design of the system. Even the organisational user framework may be affected. All these requirements need to be put down in writing and considered at an early stage.

Continued on page 58
HiWatch
Holistic Video Surveillance Solutions for Small-to-Medium-sized Enterprise

Questioning if IP, analog, or hybrid is the best security solution for your business?
Find the optimal fit for your needs here!

Hikvision, the global leader of video surveillance products and solutions, manufactures a wide range of top-quality, reliable, and professional solutions. Our solutions are designed to fit any size, configuration, location or budget that a customer might request. Case in point is the introduction of our new HiWatch video surveillance solutions specifically designed for small-to-medium-sized enterprises. With notable features, such as ease of use, maintenance simplicity, and in-time upgrading; the HiWatch solution includes a complete and affordable product line ranging from the conventional analog system to cutting-edge IP video management. Additionally, HiWatch is extremely flexible and can be combined to create optimized high-quality systems to match your specific needs.
Continued from page 56

Determining the necessary functions

As a result of the knowledge gained from the first planning steps you can now formulate some concrete technical requirements. Basically there are two ways of proceeding from here:

(1) You could request different suppliers to develop and offer plans for technical solutions on the basis of the information you have so far. When you compare them, of course, you will see very different approaches which will be very different technically as well as in terms of price.

(2) You could specify your technical minimum requirements on the basis of your own technical knowledge of video surveillance and request different suppliers to formulate specific offers. This way you can compare the prices better, but you won’t necessarily get the best possible design for your needs, and additional costs may be incurred if you have not adequately considered or formulated all points.

The ideal seems to be to combine these two approaches with a further criteria or selection stage: Specify just the minimum technical requirements. The checklist in Figure 1 will help you do this. Now you can go to various suppliers seeking an initial quote for a price comparison. The manner in which they deal with your request will tell you if the supplier is right for you or not.

If your enquiry elicits a very brief quote and a price without any further consultation, then this supplier is only right for you if you have a strong technical background and already know very precisely what you want. If the supplier offers advice or wants to know more about your application and the practical demands on the video system, then you have found a supplier who wants to provide the best design.

Next you need to check out whether the after sales service, product quality and reliability as well as the investment security are acceptable. A video security system is a long-term investment. There should be long-term service arrangements covering devices and components for defects, and allowing for changes to system requirements or system expansions. Finally, depending on the size of the investment, it might make sense to follow up references and maybe go with short-listed suppliers to see some installations.

In the next article, Geutebrück discusses some of the technical essentials to consider in specifying and selecting a surveillance solution.

For more information contact Geutebrück, +27(0)11 867 6585, charles@geutebruck.co.za, www.geutebrueck.com

Katharina Geutebrück studied electronic engineering and worked in Italy and France before returning to the family firm in Germany, where she has been managing director since 1999. She is chair of the video technical committee of the German Association of Security System Manufacturers and Installers (BHE); a board member of the regional Association for Security at Work (VSW-NW), and is active in many security market committees.

---

<table>
<thead>
<tr>
<th>Steps</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify risks.</td>
<td>This requires not only understanding of the risk situation, the protection targets and processes of the organisation but also some imagination and vision.</td>
</tr>
<tr>
<td>For each risk: describe the possible scenario sequences.</td>
<td>Each risk should be defined as precisely as possible, in all its different forms and with all its effects.</td>
</tr>
<tr>
<td>For each scenario: define the location the scenario can or will occur.</td>
<td>Describe the particular locations which are to be covered in the pictures. These define the camera where positions and the lighting requirements.</td>
</tr>
<tr>
<td>For each location: specify the (picture) data required.</td>
<td>This determines the necessary resolution in pixels and the picture rate in frames per second.</td>
</tr>
<tr>
<td>For each scenario: specify how the occurrence of a critical event can be determined.</td>
<td>What process, with what technical aid, determines that an event is recognised (e.g. video analysis process, intruder alarm system, complaint process, etc.)? This question is very application and risk specific.</td>
</tr>
<tr>
<td>For each event: describe how the relevant persons are to be informed of the event.</td>
<td>Is there to be automatic reporting to a manned workstation (e.g. a control centre with screen display) or via another form of communication (e-mail, SMS, etc.)? Or do the relevant people find out about the event from process error reports?</td>
</tr>
<tr>
<td>For each event: specify how soon after the start of the event that it must or can be detected and handled.</td>
<td>This determines the requirements for picture recording – images have to be available for the period up to the final processing of the event (if necessary as back-up copies).</td>
</tr>
<tr>
<td>Per event: specify what reactions should and can follow (ideally with a process description).</td>
<td>This step describes the operation when there is an event: Who should have access to what information (images plus additional information from third-party systems)? What operator tools, devices and communication means will these people work with? Are application-specific search masks required? From this you can derive specifications for the user interface, for user ergonomics and convenience and for interfaces to third-party systems. Here the performance and usability of the image display is particularly critical. Many systems can only display up to four cameras on one screen with fluent movement, others use different applications for presenting live and recorded images so that it is not possible to observe the current situation and the original situation at the start of the event on the same screen, etc.</td>
</tr>
<tr>
<td>For each event: specify how reviewing and subsequent processing should be done.</td>
<td>For some types of event, recorded images can help reduce the risk of the same event happening again because they provide information on its origins and causes so that countermeasures can be introduced. In addition, in many situations image data needs to be backed-up for evidential purposes. This step determines the requirements for the operator for re-viewing and backing-up picture data.</td>
</tr>
</tbody>
</table>

General conditions. The list of general conditions determine many requirements which need to be documented individually.
See the World Effortlessly
Dahua Full HD Network Solution

Dahua full HD network surveillance solution takes your concerns into account. We build our system with easy accessibility and accountability. Specifically, the wide integration with products of other leading integrators and manufacturers makes our system even better interoperable, flexible and scalable. And, we will always be there for our customers whenever they need us.
Ramla is becoming city without violence

Project teams the national police with the city municipality to confront violence on a citywide level.

Ramla, an Israeli town centre with a population of 65,000, is located in Israel’s shore plain between Tel-Aviv and Jerusalem and in close proximity to the Ben Gurion International Airport. Founded in 716 by Muslims, the city’s current population is a blend of cultures consisting of Jews, Muslims and Christians who have lived in the city for many generations. Ramla is the capital of the central region, one of the six regions in the state of Israel supervised by the interior ministry.

Measurable reductions desired

The city of Ramla is one of the pioneers of the Israeli government’s “City without Violence” programme that was initiated in 2007 and includes 16 selected cities that will receive partial government funding for video surveillance projects. The City without Violence project teams the national police with the city municipality to achieve goals of confronting all types of violence on a citywide level.

Prior to implementing the programme, Ramla performed a survey to identify strategic locations around the city where video surveillance could help create a safer city environment. These areas included main road junctions, schools and recreation areas. Without an existing fibre infrastructure, however, Ramla had the challenge of building a surveillance network that would meet their demanding needs in an environment where cameras were widely distributed.

The Vigilant solution

Vigilant’s certificated partner Top Sky Line, designed a solution and installed 67 highly visible, outdoor cameras mounted on poles in strategic locations. The cameras were connected to Vigilant’s NetStream 2300 video encoders. The NetStream encoders use a wireless Wi-Fi network to deliver high quality D1 video resolution to the municipality’s control centre. The control centre is manned 24/7 to enable response by authorities to events and residential calls. A Vigilant NetVR 5201 located in the control centre records and stores the high quality video for a period of 21 days.

“We were looking for a quality high-end video surveillance solution that would be capable of operating over a wireless infrastructure”, stated Kobi Winter, CEO of Top Sky Line, “Vigilant’s surveillance solution is specially designed for overcoming wireless network challenges while providing the highest video quality.”

Vigilant’s NetView control centre was installed in the city control room with multiple video streams being displayed over a video wall that consists of three LCD screens. Municipality personnel use NetView command, a touch screen map-based graphical user interface, to efficiently navigate throughout the city in order to instantly view and manage live or recorded video on the NetView control centre matrix.

“Vigilant’s end-to-end video surveillance solution has exceeded our expectations in every area,” continued Winter. “The NetView command user interface is friendly and effective and it allows the municipality operators to quickly respond to events by using the city maps and geographical perspective of the installed cameras.”

As one of the first municipalities in Israel to implement a digital video surveillance system, Ramla has seen a 15% reduction in violent crime. The city is planning to increase the video surveillance system in a second phase of the project to include megapixel cameras. UTM represents Vigilant in South Africa.

For more information contact UTM Group, 0860 22 22 66, kelly@utmgroupp.co.za

Doubled recording capacity

New Axis Camera Companion released with doubled recording capacity.

The rapid evolution of the Axis Camera Companion continues with a major upgrade of the free software client that doubles the recording capacity when using SD memory cards. The new release also includes new features such as multiple user access levels and joystick support.

“Axis Camera Companion has been very well received by the market. Until November 2012 we have registered over 30,000 downloads of the software. This indicates that users really appreciate the simplicity and the HDTV image quality offered by Axis Camera Companion,” says Roy Alves, country manager, Axis communication. “By also adding support for 64 GB SDXC cards in all network video products with SD card capabilities, our customers will benefit from the doubled recording capacity, which means that each camera can record over one month of video in HDTV quality.”

In addition to support for 64 GB SDXC cards, the new version includes support for administrator, operator and viewer user access levels, so that system access for different users can be restricted. Joystick support for efficient control of Axis PTZ network cameras is also available.

Axis Camera Companion allows small business owners to use HDTV network cameras to help them clearly identify intruders, shoplifters and other incidents. Video can be viewed live and recordings played back from anywhere, onsite or remotely over the Internet. The system supports motion detection and pan/tilt/zoom control. Video clips and snapshots can be easily exported to colleagues and authorities, and the system supports third-party apps for viewing live and recorded video on leading smartphones and tablets, such as iPhone, iPad and Android.

Unlike analogue surveillance installations, Axis Camera Companion does not require a central recording device – a digital video recorder (DVR), network video recorder (NVR), or even a computer. All images are recorded onto a standard SD memory card in each camera, and the cameras keep recording even if the network fails. The cameras are powered over the network, eliminating the need for separate power cables. This reduces cost, simplifies installation, and makes the system more robust as there is no single point of failure. To further protect customers’ investments, existing analogue cameras can be integrated via video encoders.


For more information contact Axis Communications, +27 (0)11 548 6780, roy.alves@axis.com, www.axis.com

January 2013 www.securitysa.com
Reditron releases Rediview range

By Andrew Seldon.

Reditron has relaunched its in-house range of cameras and accessories.

Following the management buyout of Norbain SA, renaming the company to Reditron (as reported in Hi-Tech Security Solutions November 2012), the company has also relaunched its in-house range of cameras and accessories under the Rediview brand.

According to Reditron’s channel sales manager, MJ Oosthuizen, the cameras were designed specifically for Reditron to replace Norbain’s Vista range. The goal is to offer customers a high-quality camera range that has been well designed, but at a lower cost than the traditional market leaders.

To demonstrate its confidence in the new Rediview range, Reditron is offering a 2-year carry-in warranty. Management software for both IP and analogue devices are provided free of charge. All the devices feature a Web-based console, H.264 compression and ease of use is ranked a top priority for all models. It also offers a versatile IP67 rated mounting box that is compatible with multiple camera models. ONVIF Support is standard and onboard SD storage default on majority of the IP models.

In the analogue space, it offers the RED-DVR4 4-channel recorder with full frame rate D1 recording, remote management and USB backup, as well as the RED-DVR16 16-channel recorder with similar features.

Oosthuizen adds that the cameras are already integrated into Milestone’s and NUUO’s management software.

Reditron will also allow customers to order online. Its website has been updated to allow existing customers to log in and place orders as easily or easier than they would over the phone.

Its camera range includes 12 IP and 9 analogue cameras made up of:

- Bullet cameras with InfraRed (IR) functionality,
- Mini-dome cameras with IR,
- Vandal-resistant mini-domes, also with IR, and
- Traditional box cameras.

Some of the cameras on offer are listed below:

- Its IP mini-domes range from the weatherproof IP66-rated RVIP – DM720 1.3 megapixel (MP) products with IR functionality, to the RVIP – DM1080 2 MP HD IP vandal-proof IP camera with a Micro SD memory card slot.
- The RVIP – MD720-W incorporated wireless networking capabilities into the mini-dome product range. Micro SD onboard storage is offered as standard.
- Its two IP box cameras have similar resolutions and features as the mini-domes, and similar configurations are available for both bullet cameras, with IR, but the range also includes the RVIP – IRB3MP, a 3 MP HD IP bullet with IR capabilities.
- The RVIP – EBALL720 is a 1.3 MP HD IP eyeball camera that is IP66 rated with a Micro SD memory card slot.
- On the analogue side, the company offers the RPIR-10M, a PIR mini camera with built-in IR with a range of up to 10 metres. This is a camera with pinhole lens offering a resolution of 650TVL.
- The RSMOKE is a smoke detector covert camera with ATR mode, BLC, D-WDR, OSD, 2D/3D-DNR, DSS, DIS, E-zoom, motion detection, privacy masking, highlight compensation etc. It delivers 600TVL resolution.

More information on www.rediview.co.za.

For more information contact Reditron, 087 802 CCTV (2288), marketing@reditron.co.za, www.reditron.co.za

www.securitysa.com January 2013 61
Indian hospital security improved with surveillance

Hikvision-driven security solution provides a variety of benefits for India’s Clara Swain Hospital.

In operation for roughly one-and-a-half years, a Hikvision-driven security solution has already provided a variety of benefits for India’s Clara Swain Hospital. This hospital, located in the economically-vibrant city of Bareilly, Uttar Pradesh (a northern Indian state) was suffering from “various troublemakers and individuals that really did not have any business being inside the hospital,” explained Deepanshu Girish Gupta, MD and owner of Coral Infocom Private, the system integrator for this project.

Fortunately for the Clara Swain Hospital, Gupta’s customised solution has greatly changed this dynamic: “Now, the hospital is far more secure and a safer place for both patients and employees. Moreover, we have also seen a great improvement in employee work performance. This is directly due to the Hikvision units we have installed."

Protecting and improving

This aforementioned solution features two Hikvision components: the DS-2CC 575P-M 540 TVL Low Illumination ICR Dome Camera and the DS-8116HFI-S Standalone DVR.

About 50 individual units of the DS-2CC575P-M dome camera were placed throughout the hospital’s administrative offices, corridors, security areas, ward lobbies, operating facilities, patient waiting rooms, outpatient facilities, as well as the ICU, main entrance and emergency doors – essentially everywhere except the patient rooms. Gupta explained, “Obviously, from a privacy standpoint, we do not want cameras inside actual patient rooms. But, these patients are still secure based on the fact that the corridor areas leading to these rooms are secure.”

Since all of the cameras are indoors, and as such, in a controlled-lighting environment, the DS-2CC 575P-M proved to be the right model for this solution. In particular, its compact design allowed this camera to be an unobtrusive tool, rather than big brother looking over patients and employees. “As noted, we were able to remove individuals that should not be at the hospital, and this was vital. But, also of importance, we greatly improved employee production by allowing managers a tool to review and correct errors. This camera proved to be a non-threatening benefit in helping the hospital run more efficiently,” Gupta elaborated.

Technical features of the DS-2CC575P-M include a 1/3-inch Sony CCD, 540TVL horizontal resolution, electronic day/night, 0.1 Lux @ (F1.2, AGC ON) lighting range, and internal power synchronisation.

Eyes on the go

Hikvision’s DS-8116HFI-S Standalone DVR allowed Clara Swain’s administrators an additional element: the ability to view these Hikvision cameras while they are on the move.

Gupta explained the importance: “We chose the DS-8116HFI-S Standalone DVR primarily because of its quality and to give this customer the ability to remotely monitor cameras from their mobile phones. Due to this client’s busy schedule, they are not generally in the office, ruling out the general PC-based viewing experience. Instead, we needed to allow three or four individuals to simultaneously see the cameras on their mobiles. Hikvision’s ivms-4500 software and dual-stream technology facilitated this process.”

Furthermore, the up to 8 SATA HDD in each DS-8116HFI-S unit allows the recording space needed for a large hospital, as well as the “ability to future-proof this project,” added Gupta.

Additional features, such as up to 1024×768 VGA output resolution, dual-stream support, and up to 16-channel synchronous playback, combine to make the DS-8116HFI-S a quality DVR that allows customers a wide variety of security options.

Clara Swain as a role model

The success of Hikvision at the Clara Swain Hospital has begun a security trend for Gupta and India’s hospitals.

Recently, Coral Infocom Private. completed a similar hospital solution. Notably, Gupta was able to use lessons from the Clara Swain solution as a precedent: “The key for us is that Hikvision products work. For our customers, the success we have already enjoyed is proof that our Hikvision solutions will work for them, as well.”

For more information contact Hikvision, +86 571 8700 6060, wulin@hikvision.com, www.hikvision.com
Cyber security in 2013

By Mark Eardley.

Building an information infrastructure on an insecure foundation.

In April 1998, the director of the CIA, George Tenet, said that based on the most complex systems the world has ever known, the United States was building an information infrastructure on an insecure foundation: “We have built our future upon a capability that we have not learned how to protect. We have ignored the need to build trust into our systems. Simply hoping that someday we can add the needed security before it is too late is not a strategy.”

The clear and present danger caused by this insecure foundation was emphasised in May 2012 by the head of Interpol, Khoo Boon Hui. He said, “We have seen global financial institutions suffer from major cyber attacks on their networks and servers, with US banks purportedly losing $900 million to bank robbers but $12 billion to cyber criminals last year.”

Those figures mean that for every dollar stolen by old-fashioned bank robbers in America, $117 were stolen by cyber villains.

Local evidence for this criminal shift into IT-based crime – cybercrime – is not hard to find. In a pair of cyber thefts early in 2012, two SA banking institutions were robbed of R69.3 million. In light of the continuing rise of cybercrime, it’s clear that 2013 will see even more focus on the nature and scale of the problem and how security solutions can prevent the damage it is causing. So what is the cyber problem and what can be done about it?

Cybercrime: is it for real?
It strikes me that many people think cybercrime is make-believe and that the threat it poses is not actually real; that it’s a virtual threat in some sort of hi-tech fantasy world. The term ‘cyber’ may be partly responsible for such attitudes because it creates a perception that this particular form of crime really only belongs in the movies. This is dangerous if it makes us underestimate cybercrime’s real-world significance.

It is almost certainly causing us to underestimate the importance of introducing secure systems that create an effective barrier to the cyber problem in all its guises.

Definitions for cybercrime can also be confusing and misleading. For example, does a cybercrime have to involve the Web? Within cybercrime itself do we all understand what is meant by zero-day exploits, drive-by downloads or malware? Can it be that we are doubly confused about cybercrime because the language it uses seems so alien?

For me, any crime that uses some form of IT system is a cybercrime. Using a desktop, laptop or mobile device as part of the crime turns it into a cybercrime. If it’s digital, it’s cyber. And that provides a clue to the enormous scale of the cyber problem. Because so many of our daily activities are IT-based, the spectrum of cybercrime is very broad indeed. Consequently, we are vulnerable to cybercrime in many different ways – both as individual consumers and as corporates.

Sticking our heads in the sand is also not a strategy
If it’s digital, it’s vulnerable. That unequivocal message just about sums up where we’re at with corporate cybercrime. From electronic payments, invoicing and payroll through to financial forecasts, deal negotiations and product development, any aspect of the organisation managed digitally is vulnerable to cybercrime and needs to be protected.

Obvious and well reported cyberecrimes like fraudulent EFT payments are easy to understand both in terms of how they occur and the damage done: IT access credentials get stolen and the cyber villains transfer stolen funds to their accounts. However, the cyber theft of sensitive corporate information is perhaps not so widely understood either in terms of how it occurs or its consequences. Speaking in June 2012 at the launch of an anti-cybercrime partnership between the UK’s intelligence services and the private sector, Jonathan Davis, the head of MI5 said this about the cyber threat to corporate secrets: “One major London-listed company with which we have worked estimates that it incurred revenue losses of some £800m as a result of a hostile state cyber attack.”

Perhaps the wide-ranging and diverse nature of cybercrime contributes to even more difficulty in understanding the challenges it presents. It comes in so many different shapes and sizes, and affects so many areas of an organisation’s operation that it is hard to grasp the overall nature of the cyber threat. We hold thumbs and hope that it passes us by... Speaking about the reluctance to face the challenges of corporate cybercrime, Preet Bharara, US attorney for the Southern District of New York and the ‘top cop’ on Wall Street, said in an October 2012 interview with the Financial Times that a bank would never think twice about reporting an armed robbery.

However, corporate attitudes towards cyberecrimes are clearly quite different. In Bharara’s experience, “Companies are still waiting too long to disclose intrusions to law enforcement.” He went on to say, “The fact that you don’t have senior management and its board heavily focused on something that can be a company-ending threat is an abdication of responsibility, without question.”

Bharara’s message is clear. Cybercrime should be – but isn’t – a board-level priority in terms of what organisations are doing to protect themselves from the immense damage it is causing. Perhaps the losses caused by cybercrime are so large that they almost become meaningless and therefore non-threatening. For example, the 2011 cyber theft of over 100 million customer records from the Sony PlayStation Network showed just how serious the damage can be when Sony acknowledged that it had allocated $171 million to deal with the hack-attack on their systems. That’s over R1.5 billion...
In terms of even bigger losses, the Swiss investment bank, UBS, lost over $2.3 billion in 2011 as a result of unauthorised, unmonitored – and obviously digital – trading by a London-based employee.

**Identity fraud is a major problem**

Identity-based crime affects consumers on a daily basis and much of it is digitally-based and therefore cyber. All those phishing e-mails that we receive on a daily basis are primarily looking for one thing: usernames, PINs and passwords. Cyber villains target us with these mails because if they can con us into providing our online credentials, then they are going to rob our payment cards and our bank accounts.

But they also target organisations that hold our identity details, such as banks or insurance companies and medical aids. Personally identifiable information or PII is a valuable commodity to certain cyber villains and they steal it on an alarmingly frequent and large scale.

And it’s also important to recognise that these villains are smart villains. For example, in a May 2011 cyber theft, details of over 360 000 cardholders were stolen from the American bank, Citigroup. The bank said that the stolen PII data was limited in nature and consequently insufficient to enable transactions. Customers were not at risk since Social Security numbers, birth dates, card security codes and expiry dates were not taken.

But the reinforcements were not entirely successful. It seems that card numbers, home addresses, holders’ names and e-mail details were just a starting point for the cyber villains. Just a few weeks after the theft, Citigroup disclosed that over $2.7 million (about R24 million) had already been lost to fraudulent payments.

Closer to home, it was widely reported in November 2012 that the details of hundreds of thousands of South Africans had been stolen from PayGate, a local processor of card payments for each of SA’s four big banks as well as retailers like Woolworths.

As with Citigroup’s cyber incident, PayGate said it did not keep personal data like addresses and ID-numbers, but did store e-mail details and warned customers to be wary of phishing attacks. No need to ask why….

And we are paying a high price for all of this digital crime. Consumer-based identity fraud costs South African organisations billions of rands. According to the South African Banking Risk Information Centre, payment card fraud alone cost R505 million between January and September 2012. Mike Henderson of the credit bureau Xpert Decision Systems (XDS), says that a leading local retail group is apparently losing up to R12 million a month due to identity-based fraud.

Looking beyond card-based fraud, Henderson says that at one South African vehicle finance company, 60% of credit applications have documentation problems and 30% have fraudulent identity details.

Whether it’s cybercrime within a corporate environment or happening on a consumer level, all forms of cybercrime share a common denominator: identity theft. From corporate cyber thefts based on stolen access credentials through to payment card fraud based on stolen identities, most cybercrime is based on the villains using other people’s identities to perpetrate their crimes.

Accurate control of identity through fingerprint authentication is an obvious way to counter a multitude of cybercrimes. And the losses caused by inadequate cyber security should certainly provide sufficient motivation to address the problem from the roots up.
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>E-mail</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accsys</td>
<td>+27 (0) 11 719 8000</td>
<td><a href="mailto:pr@accsys.co.za">pr@accsys.co.za</a></td>
<td><a href="http://www.accsys.co.za">www.accsys.co.za</a></td>
<td>29</td>
</tr>
<tr>
<td>Alwinco</td>
<td>+27 (0) 71 319 4735</td>
<td><a href="mailto:aviljoen@alwinco.co.za">aviljoen@alwinco.co.za</a></td>
<td><a href="http://www.alwinco.co.za">www.alwinco.co.za</a></td>
<td>18</td>
</tr>
<tr>
<td>Axis Communications</td>
<td>+27 (0) 11 548 6780</td>
<td><a href="mailto:roy.alves@axis.com">roy.alves@axis.com</a></td>
<td><a href="http://www.axis.com">www.axis.com</a></td>
<td>60</td>
</tr>
<tr>
<td>Bidvest Magnum Technology</td>
<td>+27 (0) 11 555 4949</td>
<td><a href="mailto:kevinm@bidvestmagnum.co.za">kevinm@bidvestmagnum.co.za</a></td>
<td><a href="http://www.bidvestmagnum.co.za">www.bidvestmagnum.co.za</a></td>
<td>28,45*</td>
</tr>
<tr>
<td>Bosch Security Systems</td>
<td>+27 (0) 11 651 9600</td>
<td></td>
<td><a href="http://www.boschsecurity.co.za">www.boschsecurity.co.za</a></td>
<td>49</td>
</tr>
<tr>
<td>Camsecure</td>
<td>+27 (0) 11 781 1341</td>
<td><a href="mailto:francois@camsecure.co.za">francois@camsecure.co.za</a></td>
<td><a href="http://www.camsecure.co.za">www.camsecure.co.za</a></td>
<td>26,46</td>
</tr>
<tr>
<td>Cathexis Africa</td>
<td>+27 (0) 31 240 0800</td>
<td><a href="mailto:info@cat.co.za">info@cat.co.za</a></td>
<td><a href="http://www.cathexis.co.za">www.cathexis.co.za</a></td>
<td>29,30,32,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35,37,45</td>
</tr>
<tr>
<td>Centurion Systems</td>
<td>0860 CENTURION</td>
<td><a href="mailto:adam.butchart@centurionsystems.co.za">adam.butchart@centurionsystems.co.za</a></td>
<td><a href="http://www.centsys.com">www.centsys.com</a></td>
<td>27*</td>
</tr>
<tr>
<td>Clearline</td>
<td>+27 (0) 11 848 1100</td>
<td><a href="mailto:info@clearline.co.za">info@clearline.co.za</a></td>
<td><a href="http://www.clearline.co.za">www.clearline.co.za</a></td>
<td>9*</td>
</tr>
<tr>
<td>Comb Communications</td>
<td>+27 (0) 11 089 5800</td>
<td><a href="mailto:sales@comb-communications.com">sales@comb-communications.com</a></td>
<td><a href="http://www.comb-communications.com">www.comb-communications.com</a></td>
<td>15*</td>
</tr>
<tr>
<td>Crown Hyper World</td>
<td>+27 (0) 11 830 1452</td>
<td><a href="mailto:info@crownhypper.co.za">info@crownhypper.co.za</a></td>
<td><a href="http://www.crownhypper.co.za">www.crownhypper.co.za</a></td>
<td>31,34,61*</td>
</tr>
<tr>
<td>Dahua Technology</td>
<td>+86 571 8768 8883</td>
<td><a href="mailto:overseas@dahuatech.com">overseas@dahuatech.com</a></td>
<td><a href="http://www.dahuatech.com">www.dahuatech.com</a></td>
<td>29,30,36,59*</td>
</tr>
<tr>
<td>Elvey Security Technologies</td>
<td>+27 (0) 11 401 6700</td>
<td><a href="mailto:info@elvey.co.za">info@elvey.co.za</a></td>
<td><a href="http://www.elvey.co.za">www.elvey.co.za</a></td>
<td>29,31,33,41,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>43*,44,50*</td>
</tr>
<tr>
<td>EOH Intelligent Infrastructure</td>
<td>0861 500 500</td>
<td><a href="mailto:sales.ii@eoh.co.za">sales.ii@eoh.co.za</a></td>
<td><a href="http://www.eohii.co.za">www.eohii.co.za</a></td>
<td>26</td>
</tr>
<tr>
<td>ERS Biometrics</td>
<td>+27 (0) 10 593 0593</td>
<td><a href="mailto:sales@ersbiometrics.co.za">sales@ersbiometrics.co.za</a></td>
<td><a href="http://www.ersbiometrics.co.za">www.ersbiometrics.co.za</a></td>
<td>30</td>
</tr>
<tr>
<td>Geutebrück</td>
<td>+27 (0) 11 867 6585</td>
<td><a href="mailto:charles@geutebruck.co.za">charles@geutebruck.co.za</a></td>
<td><a href="http://www.geutebruck.com">www.geutebruck.com</a></td>
<td>56,58</td>
</tr>
<tr>
<td>GSC Systems</td>
<td>+27 (0) 21 712 5130</td>
<td><a href="mailto:erich@gsc.co.za">erich@gsc.co.za</a></td>
<td><a href="http://www.gscsystems.com">www.gscsystems.com</a></td>
<td>35*</td>
</tr>
<tr>
<td>Hikvision</td>
<td>+86 571 8807 5998</td>
<td><a href="mailto:overseasbusiness@hikvision.com">overseasbusiness@hikvision.com</a></td>
<td><a href="http://www.hikvision.com">www.hikvision.com</a></td>
<td>57*,62</td>
</tr>
<tr>
<td>HomeIQ (Comfort)</td>
<td>0861 466 347</td>
<td><a href="mailto:sales@homeiq.co.za">sales@homeiq.co.za</a></td>
<td><a href="http://www.homeiq.co.za">www.homeiq.co.za</a></td>
<td>40*,41</td>
</tr>
<tr>
<td>IAC</td>
<td>+27 (0) 12 657 3600</td>
<td><a href="mailto:raine@iacontrol.co.za">raine@iacontrol.co.za</a></td>
<td><a href="http://www.iaconline.co.za">www.iaconline.co.za</a></td>
<td>33*</td>
</tr>
<tr>
<td>iFacts</td>
<td>+27 (0) 82 600 8225</td>
<td><a href="mailto:jenny@ifacts.co.za">jenny@ifacts.co.za</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inhep Electronics Holdings</td>
<td>+27 (0) 31 705 1373</td>
<td><a href="mailto:info@inhep.com">info@inhep.com</a></td>
<td><a href="http://www.idsprotect.com">www.idsprotect.com</a></td>
<td>47*</td>
</tr>
<tr>
<td>ISS South Africa</td>
<td>+27 (0) 83 330 8767</td>
<td><a href="mailto:eugene.kayat@isscctv.com">eugene.kayat@isscctv.com</a></td>
<td><a href="http://www.isscctv.com">www.isscctv.com</a></td>
<td>47</td>
</tr>
<tr>
<td>Jasco Security Solutions</td>
<td>+27 (0) 11 894 7127</td>
<td><a href="mailto:sales@multivid.co.za">sales@multivid.co.za</a></td>
<td><a href="http://www.jasco.co.za">www.jasco.co.za</a></td>
<td>27,OBC*</td>
</tr>
<tr>
<td>Keep Access Control Systems</td>
<td>+27 (0) 11 805 0175</td>
<td><a href="mailto:siska@keepacs.co.za">siska@keepacs.co.za</a></td>
<td><a href="http://www.keepacs.co.za">www.keepacs.co.za</a></td>
<td>34,36,44</td>
</tr>
<tr>
<td>Leaderware</td>
<td>+27 (0) 11 787 7811</td>
<td><a href="mailto:sales@leaderware.com">sales@leaderware.com</a></td>
<td><a href="http://www.leaderware.com">www.leaderware.com</a></td>
<td>4*,14</td>
</tr>
<tr>
<td>neaMetrics</td>
<td>0861 632 638</td>
<td><a href="mailto:info@neaometrics.com">info@neaometrics.com</a></td>
<td><a href="http://www.neaometrics.com">www.neaometrics.com</a></td>
<td>51*,53*</td>
</tr>
<tr>
<td>Physical Risk</td>
<td>+27 (0) 21 851 2963</td>
<td><a href="mailto:info@physicalrisk.com">info@physicalrisk.com</a></td>
<td><a href="http://www.physicalrisk.com">www.physicalrisk.com</a></td>
<td>20,28*</td>
</tr>
<tr>
<td>Progroup</td>
<td>+27 (0) 11 493 1545</td>
<td><a href="mailto:sales@progroup.co.za">sales@progroup.co.za</a></td>
<td><a href="http://www.progroup.co.za">www.progroup.co.za</a></td>
<td>31</td>
</tr>
<tr>
<td>PSS</td>
<td>+27 (0) 11 608 4259</td>
<td><a href="mailto:sales@pss.co.za">sales@pss.co.za</a></td>
<td><a href="http://www.pss.co.za">www.pss.co.za</a></td>
<td>17</td>
</tr>
<tr>
<td>RBE Stationery Manufacturers</td>
<td>+27 (0) 11 793 7321</td>
<td><a href="mailto:sales@rbe.co.za">sales@rbe.co.za</a></td>
<td><a href="http://www.rbe.co.za">www.rbe.co.za</a></td>
<td>16*,35</td>
</tr>
<tr>
<td>Reditron</td>
<td>087 802 CCTV (2288)</td>
<td><a href="mailto:marketing@reditron.co.za">marketing@reditron.co.za</a></td>
<td><a href="http://www.reditron.co.za">www.reditron.co.za</a></td>
<td>61</td>
</tr>
<tr>
<td>Regal Security Distributors</td>
<td>+27 (0) 11 553 3300</td>
<td><a href="mailto:info@regalsecurity.co.za">info@regalsecurity.co.za</a></td>
<td><a href="http://www.regalsecurity.co.za">www.regalsecurity.co.za</a></td>
<td>23*,30</td>
</tr>
<tr>
<td>Suprema</td>
<td>+27 (0) 11 781 9964</td>
<td><a href="mailto:enquiry@suprema.co.za">enquiry@suprema.co.za</a></td>
<td><a href="http://www.suprema.co.za">www.suprema.co.za</a></td>
<td>51*,53*</td>
</tr>
<tr>
<td>Technews Publishing</td>
<td>+27 (0) 11 543 5800</td>
<td><a href="mailto:vivienne@technews.co.za">vivienne@technews.co.za</a></td>
<td><a href="http://www.technews.co.za">www.technews.co.za</a></td>
<td>19</td>
</tr>
<tr>
<td>Technews Publishing</td>
<td>+27 (0) 11 543 5800</td>
<td><a href="mailto:justin@technews.co.za">justin@technews.co.za</a></td>
<td><a href="http://www.technews.co.za">www.technews.co.za</a></td>
<td>64*</td>
</tr>
<tr>
<td>Transaction Control Technologies (TCT)</td>
<td>0861 SMOKEM (766 536)</td>
<td><a href="mailto:sales@tct.co.za">sales@tct.co.za</a></td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>Turnstar Systems</td>
<td>+27 (0) 11 786 1633</td>
<td><a href="mailto:info@turnstar.co.za">info@turnstar.co.za</a></td>
<td><a href="http://www.turnstar.co.za">www.turnstar.co.za</a></td>
<td>13*</td>
</tr>
<tr>
<td>Tyco Security Products</td>
<td>+27 (0) 82 566 5274</td>
<td><a href="mailto:emallett@tycoint.com">emallett@tycoint.com</a></td>
<td><a href="http://www.americandynamics.net">www.americandynamics.net</a></td>
<td>3*,32,33,35</td>
</tr>
<tr>
<td>UBM Montgomery</td>
<td>+27 (0) 11 835 1565</td>
<td><a href="mailto:rosscc@specialised.com">rosscc@specialised.com</a></td>
<td><a href="http://www.ufseca.com">www.ufseca.com</a></td>
<td>23*</td>
</tr>
<tr>
<td>UBM Montgomery West Africa</td>
<td>+27 (0) 11 835 1565</td>
<td><a href="mailto:jacquess@montgomeryafrica.com">jacquess@montgomeryafrica.com</a></td>
<td><a href="http://www.ufseca.com">www.ufseca.com</a></td>
<td>5*</td>
</tr>
<tr>
<td>UTM Group</td>
<td>0860 22 22 66</td>
<td><a href="mailto:kelly@utmgrou.co.za">kelly@utmgrou.co.za</a></td>
<td><a href="http://www.utmgrou.co.za">www.utmgrou.co.za</a></td>
<td>IFC*,28,60</td>
</tr>
<tr>
<td>Viasys Intelligent Video Africa</td>
<td>+27 (0) 11 465 4549</td>
<td><a href="mailto:africa@viasys-iv.com">africa@viasys-iv.com</a></td>
<td><a href="http://www.viasys-iv.com">www.viasys-iv.com</a></td>
<td>11*</td>
</tr>
<tr>
<td>VideoIQ Africa</td>
<td>0861 VIDEOIQ</td>
<td><a href="mailto:info@videoiq.co.za">info@videoiq.co.za</a></td>
<td><a href="http://www.videoiq.co.za">www.videoiq.co.za</a></td>
<td>43</td>
</tr>
<tr>
<td>VideoIQ Africa</td>
<td>+27 (0) 82 789 2010</td>
<td><a href="mailto:info@videoiq.co.za">info@videoiq.co.za</a></td>
<td><a href="http://www.videoiq.co.za">www.videoiq.co.za</a></td>
<td>46*</td>
</tr>
<tr>
<td>ZKTeco (SA)</td>
<td>+27 (0) 12 259 1047</td>
<td><a href="mailto:hendrik@zktgeo.co.za">hendrik@zktgeo.co.za</a></td>
<td><a href="http://www.zkteco.co.za">www.zkteco.co.za</a></td>
<td>OFC*,22</td>
</tr>
</tbody>
</table>

For more information on these and other suppliers please see www.hsbd.co.za

www.securitysa.com January 2013 IBC
SECURITY TECHNOLOGY & INTEGRATION

SMART SECURITY SOLUTIONS
- CCTV
- Access Control
- Intruder Detection
- Fire Solutions
- Control Rooms
- Monitoring
- Maintenance & Service
- Flexible Finance

Tel: +27 11 894 7127  
Technical Support: 080 000 1446  
E-mail: sales@multivid.co.za  
www.multivid.co.za  
www.jasco.co.za