LET THERMAL TECHNOLOGY ALERT YOU!

Hikvision thermal cameras capture sharp images in the distance

Hikvision Thermal Cameras provide superior long-range Smart behavior analyses including line-crossing detection and intrusion detection in open and expansive areas, delivering vivid images at resolutions of up to 640 x 512 pixels. These powerful features make it the perfect solution for 24/7 perimeter protection, unhindered by any weather or light condition. Its temperature-anomaly and fire detection effectively prevent emergencies in critical infrastructure and many other applications.

Hikvision thermal products come with various styles for different application needs, including bullet, PTZ dome, handheld models and positioning system, dual-lens model with thermal and optical imaging in one unit is available as well.
## REGULARS

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>From the editor’s desk</td>
</tr>
<tr>
<td>04</td>
<td>Calendar of events</td>
</tr>
<tr>
<td>06</td>
<td>News &amp; events</td>
</tr>
<tr>
<td>11</td>
<td>Associations</td>
</tr>
<tr>
<td>13</td>
<td>Training</td>
</tr>
<tr>
<td>16</td>
<td>System integrators’ profiles</td>
</tr>
<tr>
<td>65</td>
<td>Communications</td>
</tr>
<tr>
<td>66</td>
<td>CCTV, surveillance &amp; remote monitoring</td>
</tr>
<tr>
<td>69</td>
<td>Integrated solutions</td>
</tr>
<tr>
<td>70</td>
<td>Access control &amp; identity management</td>
</tr>
<tr>
<td>72</td>
<td>Perimeter security, alarms &amp; intruder detection</td>
</tr>
<tr>
<td>73</td>
<td>Product news</td>
</tr>
</tbody>
</table>

## FEATURES

### Opinion

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Using large display screens for effective CCTV surveillance. Dr Craig Donald argues that a bigger screen doesn't always mean better surveillance.</td>
</tr>
</tbody>
</table>

### Sector focus: Smart/safe cities

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Safe cities are a prerequisite for smart cities, but the journey is long and complex.</td>
</tr>
</tbody>
</table>

### Sector focus: Security in education

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>Fees may have to fall, but education should never be compromised.</td>
</tr>
</tbody>
</table>

### Fire & safety

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>Fire safety is a critical component of any security installation, but how often is it a matter of doing as little as possible, as cheaply as possible?</td>
</tr>
</tbody>
</table>

### Licence plate recognition

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>Local is lekker when it comes to automated licence plate recognition.</td>
</tr>
</tbody>
</table>

### Security trends for 2017

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>Security systems are creating value for the organisation that goes beyond safety and securing assets.</td>
</tr>
</tbody>
</table>

### Cyber security

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>Being held for ransom is no longer something that only happens to others.</td>
</tr>
</tbody>
</table>
A place for old men?

I received an interesting email from someone in the industry recently lamenting the lack of young people involved in the security world. The individual was concerned that the vast majority of the people involved in security associations and leading security teams and/or companies were way over 40 years old – most of them over the 50 mark.

So where are the young people these days? The security industry is an enormous employer in South Africa, but are all the companies and associations really populated and run by older people?

It stands to reason that before becoming involved in associations and companies, someone would need to gain some experience in the industry. But wouldn’t networking and being involved in the background activities of the industry give younger people more options in terms of expanding their horizons?

Is it perhaps that physical security isn’t the cool place to be? While there are good margins to be made in certain areas, other areas are fiercely competitive with tight margins unless you are willing to cheat your employees and customers. Is that the reason for the lack of younger industry leaders – there’s more money in other industries or sectors?

Could the problem be that there are younger people getting involved, but they see no benefit in becoming part of industry associations because they feel there is no real value to them at the end of the day? There are some associations that exist for the sake of existing, but there are also many that are focused on their sector of the market, or the market as a whole and are working to improve the industry, the service it delivers and its overall image.

As we have seen on many occasions, the industry needs associations to set the standards and speak to government to ensure standards in skills and services. So what is the route to getting more people, and associations because they feel there is no advantage of by unscrupulous operators.

PSiRA will be embarking on a transformation drive during this year and the industry needs to be able to engage and find common ground. One company can’t do it alone and we therefore need organisations and associations that fairly represent the industry and its various segments.

Relying on the benefit that security is a must-have in South Africa and therefore a grudge purchase only results in price wars and poor service. If the customer does not see the value in spending money they will always opt for the cheapest quote – just look at the CCTV industry for proof of this.

It’s only by everyone working together that the industry can improve its image by ensuring standards in skills and services. So what is the route to getting more people, and the younger generations specifically, involved beyond their own jobs or businesses? The industry needs the experience of the old and the passion and vision of the young to move everyone forward.

Andrew
Visualize every detail in its original and natural form
180° panoramic camera without image distortion

Features
- 3 sensors in 1 camera and 1 IP address
- Seamless splicing technology for perfect image presentation
- 180° viewing angle without image distortion
- Easy installation to save cost both in cabling and labor cost
- All models come with IP67 & IK 10, designed for outdoor application
Elvey's Permaconn launch roadshow
February 2017
Elvey's newly acquired product range from Permaconn will be showcased in Johannesburg, Cape Town and Durban. The range offers a clear set of differentiating factors from the current GPRS transmitters available in South Africa. Join Elvey for breakfast and explore why Permaconn may very well be your next purchase.
For more information contact Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za, www.elvey.co.za.

UTC Technology Roadshow
February & March 2017
UTC Fire & Security Inaugural Technology Roadshow will be held early 2017 in Cape Town, Johannesburg and Durban with the aim of bringing UTC Fire & Security, closer to its customers through interaction with the relevant product managers including live product demos, Q&A sessions with technical staff as well as the latest product innovations and announcements. Showcasing some of the latest products in CCTV, access control, intrusion, fire detection & networking equipment, this event will be a must for partners.
For more information, contact UTC Fire & Security, +27(0)11 579 7300, utcfs.ssa@fs.utc.com

IoT Forum Africa
29-30 March 2017
Gallagher Convention Centre, Johannesburg, South Africa
Coming at a time when IoT is predicted to impact more than 20 billion people by 2020, this conference will highlight the latest products, applications and business opportunities in IoT. As IoT slowly becomes one of the most transformative technological phenomena to emerge in the 21st century, it is imperative business leaders be part of this one of a kind event.
For more information contact +27 (0)11 026 0981, events@itnewsafrica.com, www.itnewsafrica.com/iot/.

Secutech
12-14 April 2017
Taipei Nangang Exhibition Center, Taipei, Taiwan
The 20th Secutech will be held in Taiwan from the 12th to 14th April. Aiming at helping security professionals grow their business outside the box of conventional security, the 2017 edition gathers leading brands and prosperous startups to present next-gen innovations.

Intersec Saudi Arabia
2-4 May 2017
Jeddah Center for Forums & Events, Jeddah, KSA
Following the increasing demand for security equipment and services in the Kingdom of Saudi Arabia, 2017 Intersec Saudi Arabia will be launched in Jeddah in 2017.
For more information go to www.intersec-ksa.com.

IoT & Smart Expo 2017
24-25 May 2017
Johannesburg, South Africa
The second Internet of Things Africa Summit & Smart Expo will discuss the local, regional and global state of the industry with its progress, challenges and outlook.
For more information contact Clever Soko, 061 923 1466, register@iotafricasummit.net, www.iotafricasummit.net.

Securex 2017
30 May to 1 June 2017
Gallagher Convention Centre, Midrand
Leveraging 23 years of experience in the security and fire sector, the steady and unparalleled growth of the exhibition has earned Securex its reputation as Africa's leading sector trade show. Securing a stand at Securex 2017 is an investment in an increased customer footprint and extended industry recognition and reputation.
Taking place at Gallagher Convention Centre in Midrand, Johannesburg from 30 May - 01 June 2017, Securex is a seamless exhibition that brings together over 6000 visitors and over 160 exhibitors representing 13 countries.

IFSEC International
20-22 June 2017
Excel, London, UK
The leading security conference and exhibition, IFSEC International covers every aspect of security, from access control and video surveillance to smart buildings, cyber, border control and more.

ESDA 2017 Charity Golf Day
31 August 2017
Royal Johannesburg Golf Club
The ESDA 2017 Charity Golf Day will be held at the Royal Johannesburg Golf Club on Thursday 31 August 2017.
For further information or to book a 4-ball, contact shirley@esda.org.za.

Camprosa International Conference 2017
3-6 September 2017
Kwa Maritane Bush Lodge, Pilanesberg National Park, NW Province
The Campus Protection Society of Southern Africa is set to host its 2017 international conference at Kwa Maritane Bush Lodge from the 3rd to 6th September 2017.
For more information on the full programme, go to www.camprosa.co.za

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.
MORPHOACCESS® SIGMA LITE SERIES
SLIM AND POWERFUL FINGERPRINT ACCESS TERMINALS

Morpho

Morpho

- World’s #1 fingerprint technology inside
  1:10,000 user identification in 1 second
- High capacity
  30,000 templates, 250,000 IDs in authorized user list, 1 Million logs
- Anti-fraud features
  Fake finger detection, duress finger, timed anti-pass back
- Flexibility
  Prox®, iClass® or MIFARE®/DESFire®/NFC contactless card reader as an option
- Tough design
  IP65 rated and vandal resistant (IK08)

Morpho South Africa Pty Ltd
Tel +27 11 285 5800 – Fax +27 11 285 5879 – www.morpho.com – sec-san.orders@morpho.com
107 Johan Avenue Wieda Court Block B Wieda Valley Sandton 2196
PO Box 3826 Rivonia 2128 – SOUTH AFRICA
Reg No. 2005/002305/07 – VAT 4530222316

Embedded WEB SERVER
Paxton strengthens South African team

Paxton recently appointed Mark Kidd-Anderson to its business development team for South Africa. Based in Cape Town, Kidd-Anderson will support and assist distributors and installation companies in the East, West and Northern Cape regions via training and presentations. He will ensure they are aware of Paxton’s product offerings and are taking advantage of the sales opportunities available.

Kidd-Anderson joins Paxton with over 16 years experience in the security industry, previously holding roles at Elvey Security Technologies, Pentagon Distribution, Inhep Electronics and most recently Redtron.

Commenting on the appointment, Dan Drayton, country manager for Paxton, said: “We’re delighted to welcome Mark on board at what is an exciting time for the company. His depth of industry knowledge will provide great value to our customers and help accelerate our growth right across South Africa.”

Kidd-Anderson is looking forward to the challenges ahead and said: “I was introduced to Paxton two and half years ago, the company, and its range of products have never disappointed – from support to training to high level management interaction.

Paxton recently announced that its access control software, Net2 is now available licence-free and the company also offers free, hands-on installer training for its complete range of networked access control and door entry solutions.

More local support

Paxton has also announced the integration of its networked access control system, Net2, with South Africa’s Llama Consulting’s visitor management system, LlamaNET. The integration provides simple multi-platform access management for registered users, enabling them to request PIN codes for visitors via their mobile phone.

LlamaNET is a cloud-based system that uses a mobile application to bring PIN-based visitor management to Paxton’s Net2 access control. Push notifications alert the user of their visitors’ arrival and departure, and bulk push notifications allow management to communicate with all registered users at the same time. Registration and reporting take place in the admin web portal, while the user web portal is for online visitor booking. Optional fields are available to capture additional data, providing increased security, plus SMS fall back.

Founded in 2008, LlamaNET is a subdivision of Llama IT and was established to cater for the dynamic market of visitor management. With various software deployments in many different sectors of the industry, the developers at Llama pride themselves on quality software and customer satisfaction.

Wynand Gerber, LlamaNET system designer and integrator said: “The LlamaNET visitor system is a prime example of our company ethics, with ease-of-use as a primary objective. With no monthly contracts, LlamaNET is ideal for many applications including residential estates and business parks. We believe users will quickly realise why LlamaNET is such a popular visitor management platform.”

Drayton added: “At Paxton, we put our core values of simplicity and quality at the heart of everything we do. It’s a pleasure to work with Llama Consulting, a company who place as much importance as we do on supporting customers and developing innovative solutions for the security industry. We believe this new product answers the needs of the security market, and look forward to receiving feedback from our customers.”

For more information, contact Paxton, +27 (0)21 427 6691, support@paxtonaccess.co.za, www.paxtonaccess.co.za.

Promote your security training courses with a 3-in-1 approach

Training is becoming a critical function within the security industry, as can be seen by the efforts of the industry regulator to implement new training standards across the board. Security companies that want to succeed in future need to ensure that their staff, from guards to technicians to assessors and managers, are adequately skilled.

Training is not only something of importance to trainers and learners, but for the future of the industry itself. Not only are updated skills required for efficient client service as well as understanding the latest technologies designed to assist in securing people and assets, large integrators are increasingly retaining the services of smaller specialists to provide rare skills to their clients.

To effectively serve the growing need for training courses in a variety of fields pertinent to the security market, Hi-Tech Security Solutions will launch a dedicated 3 in 1 Training Platform in February 2017. This platform makes use of different media platforms to provide effective, targeted advertising exposure for security training courses.

The 3 in 1 Training Platform will be advertised in the print issues of Hi-Tech Security Solutions, on the Hi-Tech Security Solutions’ website (www.securitysa.com) and in the Training News Briefs to ensure readers know where to go for their training requirements. More specifically:

• Each issue of Hi-Tech Security Solutions will include a training section where companies offering training can advertise their courses.

• All courses listed in the print edition will be listed in the training category of the Hi-Tech Security Solutions’ website.

• A dedicated Training News Brief will be sent out once a month to a mailing list of readers who have requested information on security services, products and related information, including training. This list currently comprises over 2 800 readers and is growing steadily. If you offer training to the security industry, make sure the industry knows who you are and what you offer by taking advantage of the 3 in 1 Training Platform from Hi-Tech Security Solutions.

For more information please contact Tracy on tracy@technews.co.za or Laura on laura@technews.co.za.
In April 2016, Kenya’s education cabinet secretary, Fred Matiang’i, announced that universities and colleges will need to capture the biometric data of all students. This move is in the wake of the increased number of terror attacks in Kenya and will entail enhanced security measures that include the installation of metal detectors and the use of biometric registration systems.

On the back of this enhanced security awareness, the second SecurExpo East Africa exhibition, held at the Visa Oshwal Centre in Nairobi, Kenya between 8 and 10 November 2016, was a firm success. PowellTronics once again participated in the event and the team was suitably impressed at the calibre of visitors attending.

Mike Austen, national sales manager at PowellTronics, says that the number of exhibitors increased from 50 in 2015 to 60 in 2016. “This is indicative of the increased exposure the exhibition has experienced since its launch in 2015. We noticed that although we had fewer visitors to our stand, the purchasing ability of these visitors was much higher than in 2015. Without a doubt, the visitors were a more focused group of people and included a number of end users and installers looking for specific project solutions. We even discussed our solutions with representatives from the governmental offices of neighbouring countries as well as the Malawi High Commission.”

With the presence of Morpho and Impro at the show, the collaboration between the three companies and their dedication to and investment in the Kenyan market was highlighted.

Attending GovTech
The tenth GovTech ICT conference, held at Gallagher Convention Centre in late 2016, focused on public sector ICT service delivery. PowellTronics used the event to showcase its access control technology solutions and capabilities to a captive audience of government-employed risk and ICT managers.

GovTech is organised by SITA, the South African Government’s ICT platform. Responsible for the consolidation and coordination of the State’s information technology resources, it enables the efficient delivery of e-government services to the public, as well as overseeing the procurement and delivery of IT processes to ensure that government uses the most cost-effective services.

John Powell, CEO of PowellTronics, says that this is the second consecutive year that the company has had a presence at GovTech. “We were invited by our customer CEOS to provide a component of their Platinum sponsorship package. CEOS Technologies was responsible for the provision of turnstiles and enrolment for the conference and PowellTronics sponsored all the biometric readers at the entrance to the venue and all of the enrolment devices at the registration desk.”

PowellTronics promoted its entire range of access control solutions including door hardware and intercoms as well as hardware from Morpho and Impro. While all of the company’s software solutions were available for review, its main focus at the GovTech event was the exposure of PT Active Directory (PT-AD).

Leonie Mangold, PowellTronics Johannesburg sales consultant, says that the opportunity to leverage both CEOS presence at GovTech as well as their solid reputation in the governmental market sector, played a large role in the positive reception to PowellTronics’ offerings at the event.

“We benefited by our presence at GovTech in two respects. Firstly, the opportunity to amplify our branding was provided at the entrance and registration desks and secondly, the platform provided by being on CEOS’ exhibition stand allowed us to interact with a very targeted and niche market,” says Powell.

For more information contact PowellTronics, 0861 787 2537, marketing@powelltronics.com, www.p-tron.com.
A Wall Street Journal study of the last recession showed that companies that cut back on marketing lost sales and market share, while those that maintained their marketing increased profits when compared to those that reduced marketing (source: http://www.entrepreneurmag.co.za/).

Furthermore, Nigel Hollis, chief global analyst at Millward Brown, noted that “The connection between share of market (SOM) and share of voice (SOV) has been proven. The higher your share of voice compared to your actual market share, the more likely your brand is to grow its market share in the subsequent year. So, if you increase your marketing investment at a time when competitors are reducing theirs, you should substantially increase the saliency of your brand. This could help you establish an advantage that could be maintained for many years.” (source: http://www.millwardbrown.com/).

With a track record that spans almost a quarter of a century, Securex has established a niche as Africa’s largest security and fire exhibition. The annual event has been the platform from which hundreds of products have been launched to a receptive target audience.

“As technologies emerge and change, prospective customers who are keen on acquiring information on best practice seek out accessible ways of contacting reliable suppliers. Securex is the ideal interactive medium for the market to connect with leading manufacturers and suppliers of security and fire products and services as they evolve,” says Joshua Low, Securex Event Director at Specialised Exhibitions.

“Securex 2016 was extremely successful, with a 20% increase in visitors achieved over the three-day period. Hosted at Gallagher Convention Centre in Midrand, from 30 May to 1 June, Securex 2017 is set to continue in the tradition of past shows and we have only 35% of the planned stand space available for interested exhibitors. We have refined our visitor attractions, maintaining a number of our ever-popular ones and adding new ones based on our market research survey results,” he adds.

Visitor attractions at Securex 2017 will include the New Products Display, situated at the entrance to the exhibition, the Securex Seminar Theatre, the FPASA half-day workshop, the ESDA breakfast and the SAIDSA Techman Competition.

“In order to remain as comprehensive in our technology coverage as possible, we continually review the verticals within the security and fire sectors. For instance, this year we will showcase: access control and identity management; alarm systems and panels; CCTV and surveillance equipment; electrical and security communication and accessories; fire protection products and systems; guarding and control rooms; IT infrastructure and cyber security; perimeter and physical security; retail security; vehicle security; X-ray and body scanner equipment; training courses, and more,” Low explains.

“It is imperative that all companies engaged in the manufacturing and/or provision of security and fire products and services contact our Securex 2017 team to discuss an optimum stand position before they lose out,” Low points out.

To reserve a stand, interested companies should contact Zelda Jordaan or Grant Bydawell on: zeldaj@specialised.com or granttb@specialised.com or visit www.securex.co.za

Rob Anderson & Associates has announced that Derick Serfontein will be joining the practice in 2017 as a partner. Serfontein has had many years’ experience in the electrical consulting engineering industry, which will add much value in a time when skills and experience are in short supply.

Rob Anderson & Associates has been active as consulting electrical and security engineers for 20 years. It is anticipating the start of some exciting projects in 2017 and Serfontein will provide just the experience required to share the challenges, as well as bring along new opportunities.

It is anticipated that the company will move offices in 2017, but a final location is still to be decided. While work in Durban continues to expand up the North Coast, the office has projects in Africa, Cape Town and Gauteng.

For more information contact Rob Anderson & Associates, +27 (0)31 267 4150, rob@robanderson.co.za, www.robanderson.co.za.

The annual Security Association of South Africa (Western Cape) Charity Golf Day remains a prestigious event. The tenth golf day will be held at the Durbanville Golf Course on the 13th of March 2017. All proceeds will be donated to SASA charities – last year the organisation was able to donate R20 000 to the Bel Porto School.

The competition will be a 4 Ball Better Ball Alliance with two scores to count on all the holes. To ensure you book your place, responses are requested by 3rd March 2017. The field will be limited to 120 players and entries will be on a first come first served basis.

Each 4 ball will cost R3 000 per team, and companies entering more than one 4 ball will be eligible for a discount.

Moreover, there are additional sponsorship opportunities. Companies can sponsor a green & tee at R1 100, or one of the special holes at R1 100 (nearest to the pin, longest drive, short hole) or one of the medium holes at R550. Additionally, other sponsorships are available, such as sponsoring prizes, donations, wet holes, the halfway house and more.

For more information or for entry forms, please contact Dave Waywell on +27 (0)21 448 6390 or dave.waywell@elvey.co.za, or John Hitchcock on +27 (0)82 801 9157.
Hochiki Europe increases presence in African market

Hochiki Europe, a manufacturer of life safety solutions, has invested in its African sales team and infrastructure to capitalise on the rapidly expanding economy.

Martyn Hanks has joined Hochiki Europe to lead sales across Africa. Driven by the economic growth especially in Rwanda, Tanzania and Mozambique, the Hochiki Europe expansion recognises the increasing importance of the market to the fire and safety systems industry.

Bolstered by this appointment, Hochiki Europe has also created an online portal specifically for the African market to ensure local protocols, standards and experience can be accessed quickly for customers.

Graham Lowe, sales director Hochiki Europe, said: “With growing importance being placed on life safety systems across many countries in Africa and the reliance on Europe and America to support with initial standards, Hochiki Europe saw to bolster its 20-year commitment to the continent.

“Hanks has extensive experience working in the sub-Saharan region and will be perfectly placed to support the requirements of the market as it continues to develop.”

He has already formed good working relationships with Hochiki’s existing customers in Africa, helping to secure contracts on a number of refurbishments and new builds in the region.

For more information on Hochiki Europe’s presence in Africa please visit www.hochikieurope.com/africa.

TeleEye SA launches GoThermal.co.za

After being founded by certified thermographers and thermal imaging experts over a decade ago, TeleEye SA has now launched GoThermal.co.za.

This web portal showcases offerings within categories that include thermal devices, commercial security, outdoor, tactical, instrumentation, building, mechanical, electrical as well as unmanned aerial systems. It enables online shoppers to receive personalised advice before making a purchase.

“TeleEye SA has many years’ experience providing industries and consumers across South Africa with imaging, sensing and security products. We wanted to bring that experience to the online world while still offering the guaranteed personalised pre-sales service and after-sales support of a bricks and mortar retail store,” said TeleEye SA managing director, Philip Smerkovitz.

GoThermal’s parent company has carved out its reputation in one of the world’s most sophisticated thermal markets. TeleEye SA is the leading South African distributor of a wide range of surveillance products, FLIR thermal imaging products, DJI industrial drones and accessories, as well as Optex detection devices.

TeleEye SA has supplied thermal vision and security solutions to such flagship real-world installations as the Google-backed Jasper solar power plant in the Karoo, Eskom substations, and various mobile base stations for South Africa’s leading cellular providers. TeleEye SA’s range of heat-detecting cameras are also thermal measurement, instrument and data recorders that add tremendous value to drone operations and services. All of this advanced hardware is now available at GoThermal.co.za.

“Other reasons to confidently choose GoThermal include the fact we are an authorised FLIR security product in and out-of-warranty repair centre, we keep a constant supply of popular stock items ensuring rapid delivery, and we are certified to run thermal training courses. All of this means you really are partnering with the best in the business,” concludes Smerkovitz.

For more information contact TeleEye (South Africa), +27 (0)11 557 9200, www.TeleEye.com.

Authlogics appoints AxizWorkgroup as a distributor in Africa

Multi-factor authentication company Authlogics has announced that AxizWorkgroup is its first local distributor and will deliver authentication solutions to resellers in Africa.

“We believe that moving away from password-based authentication is inevitable and we look forward to driving the adoption of a new generation of solutions among businesses in Africa with AxizWorkgroup,” says Steven Hope, CEO of Authlogics.

Authlogics introduced the concept of one-and-a-half factor sign-on and takes advantage of the latest smartphone technology to replace costly hard-tokens with highly secure and reliable soft-tokens. Its authentication solutions are language independent, which make them particularly valuable for African businesses that serve multiple language customers.

“We are excited to offer Authlogics to our reseller base and are ready to drive implementation of this next generation authentication technology,” says Alessandro Postiglioni, business unit manager – security at AxizWorkgroup.

As an Authlogics Gold Partner, AxizWorkgroup offers resellers account and project management, specialised security skills, national logistics and delivery infrastructure. The Authlogics Partner Programme includes independent software vendors, original equipment manufacturers, system integrators and distributors who offer Authlogics authentication solutions.

The Authlogics solutions reduce the reliance on passwords, relieve pressure on the helpdesk for password resets, ensure regulatory compliance, mitigate risk and improve customer experience with simple, memorable and secure login.

For more information visit www.axizworkgroup.com.
Keeping ahead of the competition

By Andrew Seldon.

Impro hosted a breakfast at the end of 2016 in which the company highlighted its history, the products and solutions it is bringing to market, as well as how the company is progressing since the buyout by ASSA ABLOY.

Impro’s MD, Errol East started proceedings with a quick overview of the company from the formation of Digital Controls in 1982 to the current business. He highlighted various products the company released over the years, showing how technology has advanced and how Impro has incorporated these advances into its products.

East touched on a few pertinent inflection points in the company, such as its adoption of the OS/2 operating system in the ‘90s, which turned out to be a mistake. He also mentioned the company’s development expertise and the move to Agile Development principles in the late ‘90s and early 2000s. Agile Development sees companies making continual improvements through small incremental changes instead of massive new releases at distant intervals.

He said one of the biggest lessons learned over the years is that one has to make products that are reliable and dependable. You can’t expect customers to remain loyal if they are continually facing poorly performing or breaking products.

The IXP range is an example of one of the innovations from Impro, initially released in 1999. Today, all its historical development and innovations are built into the company’s current Access Portal solutions. The new range was the result of a complete redesign of the company’s products a few years ago, part of Impro’s drive to keep pace with changes in the industry and the market at large.

At the same time, Impro is not abandoning its customers using older products which have a long lifespan as a result of the quality in the company’s design and manufacturing processes. East is adamant that Impro should continue to control its production to ensure the quality of the solutions ending up in customers’ hands.

This will not change with the ASSA ABLOY acquisition. East says the company’s new parent offers Impro access to a broad range of intellectual property and global expertise in a variety of fields, but it expects Impro to continue operations as normal. ASSA ABLOY buys into winning solutions, but then allows the company to continue its successful operations while giving it a broader scale in which to operate.

The power of Portal

Following East, Linda Glieman, head of client services at Impro took the floor to briefly discuss some of the newest solutions from the company. She highlighted the Portal solution and the benefits of real-time business intelligence it provides, as well as how the platform has been enhanced, for example, enabling clustering in larger installations. The customisable Portal Dashboard, a live web-based solution was also demonstrated, along with Impro’s visitor management solutions.

Impro’s ability to integrate with other systems in the market was also demonstrated, such as the work the company has done with Morpho readers, Nedap long-range readers and Aperio electronic locks. Impro has also adopted HID Global’s mobility applications which allow users to keep their access and identity credentials on their smartphones.

For more information contact Impro Technologies, +27 (0)31 717 0700, vikkiv@impro.net, www.impro.net.

New investment and drive for GeoVision SA

By Andrew Seldon.

GeoVision SA has announced that the Dölberg Group has invested in the company. The new equity partner will ensure that GeoVision SA makes an impact on the local market in 2017 with a number of enhanced services it can now offer.

An immediate benefit for the market is that GeoVision SA will now be able to hold more stock locally, cutting lead times significantly for installers and integrators. The company will also be able to offer better pricing due to the negotiating strength of the Dölberg Group.

Jacques Taylor, sales manager at GeoVision SA notes that another benefit partners will receive is a new 5-year product warranty (subject to terms and conditions), along with the continued 24-hour telephonic support service. Not only does this demonstrate the confidence the company has in the quality of its products, but it also sets the company apart in a market where all too often the cheapest products win the deal.

“With improved pricing and the 5-year warranty, we are setting a standard in the mid- to high-end market where performance and reliability counts,” states Taylor.

GeoVision SA will now also include a range of financial options to assist buyers in making the most of their cash flow without compromising their security and surveillance budget.

“GeoVision SA is now in a position to offer very attractive financing and/or rental options to our customers, with the financial backing and long-term experience of Dölberg,” adds Taylor. “What’s more, we are also expanding our scope of operations and addressing a wider range of business sectors than ever, offering intelligent solutions that deliver real value without negatively impacting our customers’ cash flow.”

Heinrich Odendaal, chairman of the Dölberg Group, said the partnership will bring a host of exciting opportunities to the security and surveillance sector, making the acquisition of reliable and intelligent security solutions more affordable to a broader range of companies.

For more information contact GeoVision SA, +27 (0)12 664 0411, sales@geovisionsa.co.za, www.geovisionsa.co.za.
Late last year, the Private Security Industry Regulatory Authority (PSiRA) held a conference at the Midrand Conference Centre to deliver an update on its performance during the 2015/16 financial year.

The keynote speakers were chairperson Professor Fikile M. Mazibuko, director Manabela Chauke, chief financial officer Matlou Sibogodi, acting deputy director (law enforcement) Stefan Badenhost and deputy director (CRM) Mpho Mofikoe.

Professor Mazibuko stressed that performance was a significant part of the advances made by the organisation. "This event is to celebrate the stability, growth and achievements of year 2015 and 2016 for PSiRA. These were done through committing and eradicating average service and replacing them with excellence, and delivering of quality service to the industry. We managed this through the criticisms, questioning and by being held responsible by the industry’s experts. In the process, we learnt a lot as an organisation.

"I am currently working with my team in putting together a Transformation Charter for the industry, which will help add some substance to the contribution of the organisation."

Chauke gave an overview of the organisation’s progress in what he deemed “from tough times to normal times”. He said, "We are proud to have achieved an unqualified audit opinion by the Auditor General of South Africa in 2015/16. That just shows how well we prioritised our collection of monies and how we were responsible in our expenditure as a regulator, taking into account that we are not state funded."

"In that same light one has to look at the organisation's background. From 2010 to 2012 our priority was a turnaround strategy. Then in 2013 we put forth an emergency action plan. We entered negotiations with industry and faced challenges in court, but finally came to terms with industry. And in 2015 and 2016 we adopted the normalisation strategy where we focused on the stability of the business."

A brief background was provided as to how PSiRA managed to sustain itself and achieve a clean audit by CFO Matlou Sibogodi (refer to the PSiRA Annual Report 2015/16). Acting deputy director (law enforcement) Stefan Badenhost highlighted on how the organisation faired on issues of law enforcement with those in the industry that did not comply.

Deputy director (CRM) Mpho Mofikoe, who also acted as the programme director, concluded the business of the day by underlining how important it was for industry training providers to register with PSiRA and to comply.

For more information contact PSiRA (Private Security Industry Regulatory Authority), +27 (0)12 003 0500/1, info@psira.co.za, www.psira.co.za.
There is a need for some sort of rules, written or verbal, if a group of people is to live harmoniously together. It is to this end that the FDIA was formed in 1999, to provide some guidelines and self-regulation in the industry where companies conduct their business in the field of the installation of fire detection and suppression systems. The FDIA is continuously uplifting the standards in the industry by the various functions and services the association provides to its members and the industry at large.

Membership is open to any company which gains its income from, or has an interest in, the supply, design, installation or servicing of fire detection systems, gaseous extinguishing systems or evacuation systems. Membership to the FDIA is for companies and not individuals. The FDIA website www.fdia.co.za provides the requirements and cost implications for companies wishing to join the association or maintain their membership with the association.

Members are provided with the current standards in the industry and encouraged to attend the various approved and accredited training courses that are available all year round. Each year in February, the FDIA holds its Annual General Meeting (AGM) where new committee members are elected and the various issues affecting the association and industry are discussed and deliberated upon.

The FDIA has in the recent past made it easier for new companies to join the association by requiring only one inspection of their installation to be carried out, instead of three inspections as was previously the case. Although after joining one must still have at least three inspections done in order to renew and maintain the membership.

Inspections for fire detection and suppression installations are an important aspect to obtain and maintain FDIA membership though it can sometimes be a daunting experience for companies, it is akin to sitting for an exam or going for a job interview. The main reason for inspections is to ensure that the installation is up to standard and the system will work as it was intended.

If there are any non-compliances, either minor or major ones, they are noted in the report issued to the installer and the installer is advised on how to rectify them. The FDIA is in the process of considering a service division for companies that are doing more of service/maintenance work than installations. The service division inspections will ensure that systems are serviced and maintained as per the required standards.

The FDIA has also been regularly sending out newsletters to its members, consultants in the industry and interested end-users, to keep them updated on developments in the industry on various topics regarding fire detection and suppression systems.

FDIA members recognise the responsibility to have integrity and maintain high standards of the work they do which is to protect life and property by the systems that are being installed. That is why all members are required to abide by a code of ethics which they receive and sign on acceptance of membership.

The benefits for companies to become FDIA members is therefore evident as it most importantly shows the seriousness and commitment that a company has for the work they are doing.

The benefits for end-users is even greater when they use the services of FDIA registered members as they are guaranteed that they are getting value for their money. The risk involved in using a non-FDIA company is much greater than the money one may think they are saving by using a company that does not have to abide to any code of ethics or follow any standards or rules.

We therefore encourage companies that are installing fire detection and suppression systems to take a step in the right direction and make an effort to join the association. We currently have a membership of 44 companies and several pending applications. Membership is increasing as more companies realise and appreciate the benefits of becoming an FDIA member company.

End users and consultants have seen the quality of work and integrity of FDIA member companies and they prefer to use companies that have an active membership with the FDIA.

Feel free to contact FDIA via email fdia@fdia.co.za.
TRAINING

Technical Surveillance Countermeasures (TSCM) Training courses

Course dates: Variable
Venue: Centurion, Gauteng

Description:
EDS is presenting a number of TSCM training opportunities in 2017. All training takes place at the EDS-TSCM Training Academy in Centurion, Pretoria. High-quality training according to international standards in a dedicated training facility.

For more information contact:
Eavesdropping Detection Solutions (EDS), Steve Whitehead,
+27 (0)12 665 2109
training@tscm-za.com
http://www.tscm-za.com/training.html

CCTV surveillance skills and body language training

Course dates: Variable
Venue: Throughout southern Africa

Description:
A 2-day course using extensive video incident material to show key learning points. The course is ideal for managers, supervisors, operators and investigators involved in CCTV surveillance or analysing video footage. Each course is personally trained by Dr Craig Donald.

For more information contact:
Leaderware, Dr Craig Donald,
+27 (0)11 787 7811
sales@leaderware.com
www.leaderware.com

DSC Neo Wiring & Basic Programming

Course dates: 14 February – 15 February 2017
Venue: Elvey Head Office

Description:
The course will introduce the learner to the DSC Neo system and all related programs. You will also learn the skill required to program the system. The course will be spread over two days and is perfect for technicians.

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

SAIDSA Certified Technician

Course dates: Variable
Venue: Johannesburg, Gauteng

Description:
5-day certified technician, generic training course.

For more information contact:
SAIDSA, Cheryl Ogle,
+27 (0)11 845 4870
saidsa@mweb.co.za
www.saidsa.co.za

Advertise your security training courses

in the training section of Hi-Tech Security Solutions

in print electronic newsbriefs online

Contact vivienne@technews.co.za for details

www.securitysa.com February 2017 13
Using large display screens for effective CCTV surveillance

By Dr Craig Donald.

A bigger screen doesn’t mean better surveillance.

At one of the first security exhibitions I attended a number of years ago, CCTV technology had been enabled to display multiple multiplexed camera views on single monitors. Almost every stand had demonstrations of how one could have four, nine or even an unbelievable (for those days) 12 cameras displayed on a single monitor.

Most of these displayed on 14-inch or 15-inch monitors, although some were showing these on the new 19-inch monitors that were the state-of-the-art then. My overwhelming impression and concern at the time was how small the individually displayed camera views were and what could be usefully seen on them.

Now, years later, the screens have got larger with 55-inch or even bigger TV screens being almost commonplace in control rooms, the resolutions have got higher than the VGA or SVGA that we had then, and the display technology has advanced exponentially. What hasn’t changed though, are technical installers and software developers mission to display as many camera views on these display screens as possible. The problem of identifying any meaningful behavioural signals or details on camera views has just got bigger along with the displays, shown with more brightness and resolution, and more complicated because there are now 32 instead of four or nine camera views displayed.

Using large flat screens is becoming increasingly popular within control rooms rather than using multiple monitors to show different camera views. Similarly, using multiple large screens to have a monitor wall is also relatively common, especially in high-end operations. Using large screen displays allows you to incorporate information from multiple cameras as well as control displays in a common area. However, having the screens themselves does not necessarily provide the answer.

Form and function

We hear how form should follow function and as far as CCTV is concerned, this means that your control room design and layout should follow the type of surveillance you are doing. The type of monitor configuration will vary if you are reliant on alarm-based activation, viewing traffic conditions and congestion, checking access to a particular area, or looking for theft conditions of sensitive products.

The number of cameras you are looking at, the priority of showing different camera views, the time things are displayed, are all important factors. But the most critical aspect to displaying camera images in the control room is whether it is possible to detect the type of incident behaviour you are looking for and retrieve appropriate information. For example, detecting a group of people in an area may be one thing, but identifying the actions of a pickpocket within the group requires a much larger view of potential critical behaviour.

Similarly, seeing a car in an lane set aside exclusively for buses is one thing, but being able to identify the registration number for a police response is another. Monitoring people entering a bank can be simply done with a relatively small image, but seeing whether they are carrying weapons may be impossible when viewing the same size picture. Like any display technology, camera views need to be of a sufficient size to suit the viewing objectives and tasks.

How long is a piece of string?

I am often asked how many camera views can be displayed on a large visual display. It is similar in a way to the question of how many camera views can an operator monitor, whether they are separate displays or on one large display. This question misses the main point though.

The simpler questions are can you see what you are looking for in the camera image, and does the size of the image allow you to detect relevant conditions? Fortunately, the way to test this is incredibly easy although seldom practiced. The manager and other staff including the technical personnel should sit down in the
operator's chair, and see if they could do exactly what they expect of the operator. If they can't, the answer is the camera view displayed is simply too small for the monitoring task.

Large flat screens and modern video management systems potentially have major benefits in allowing different configurations of what is to be displayed on the monitors. In fact, this customisability should be an integral part of how you choose the systems on your site. However, such a configuration should be based on a number of aspects instead of whether you display 12, 20 or 30 camera views on the system. These include:

- The ability to size a subset of camera views that are larger than the others.
- Having a large camera view similar to a 'spot monitor' to enable closer analysis of what is happening. This should be easily switchable to view different cameras.
- The ability to drag and drop cameras to specific locations on the screen.
- An operational interface that allows easy camera selection within a defined viewing layout and doesn't crowd out the effective viewing area.
- Macro settings that allow you to switch the cameras and interfaces according to specific times of day when camera or viewing priorities change, or when specific events occur.
- Configuration of the display view to allow live monitoring and well as reviewing specific camera views is something that is uncommon on systems, but could be useful for various viewing situations. In some X-ray systems, for example, you have reference images that allow you to view a previous scan of a person, in order to do a direct comparison and assist in interpreting anomalies. This kind of feature can be equally relevant in CCTV situations.
- Being able to save a range of screen configurations to deal with different conditions and situations.

A problem with large screens has traditionally been the distance from the screen to the viewer. Anyone who views a 50-inch TV with their favourite series from 1 m away is going to have difficulties in seeing things properly and will probably end up with a headache after some viewing time. However, with a large display showing multiple elements, this problem is reduced.

The size of the elements being viewed at any one time is typically the same size as in using smaller monitors. The only problem under these conditions is that the operator may need to have a high use of peripheral vision as there are multiple elements that need to be covered across a wide viewing area.

Grouping relevant camera views together under such conditions is important, as well as having operational controls well positioned relative to viewing areas. For instance, having to use a mouse-based onscreen control for a PTZ that is positioned in the top right hand corner to control a camera view on the left hand side of a 50-inch display becomes exceedingly difficult.

Large screens do have a number of advantages in viewing scenes. From the point of view of a single workstation, a number of camera views can be grouped and managed, are accessible and easily viewed. There can at times be issues relating to effects such as lighting differences and border definition, as well as the issues relating to camera selection.

Sometimes even the more expensive video management systems have poor human interfaces that make effective control and customisation difficult. There is still a role for separate monitors though, particularly when only a small selection of specific camera views are needed, or to complement a large screen. Separate monitors are also often necessary when different control systems are used.

Additionally, when you start putting more than one large screen in front of operators, it substantially increases line of sight issues, with either a very wide line of view where things can occur out of sight on the periphery, or the vertical line of sight where operators have to lean back or tilt their necks excessively in order to see anything on the additional large screen. Nevertheless, we can expect large screens to increasingly become a more integral part of CCTV systems.
Integrated infrastructure solution for financial services firm

By Brett van den Bosch.

BT-SA recently completed the installation of an all-inclusive infrastructure solution for a major client’s new administration building and workshop.

Although the client in question cannot be named due to the sensitive nature of its operations, BT-SA’s managing director, Erik Jordaan, describes it as a local financial and investment services holding company which owns a number of buildings in an upscale business park in the east of Pretoria. The tenants are involved in a wide range of forensics that includes digital forensics and also prepaid electricity meter management solutions. Having completed the initial project, BT-SA has embarked on the design phase for the next three buildings in the business park.

BT-SA was involved in the project since the design and together with the architects and designers ensured all elements, products and installation conformed to the highest standards. The company was responsible for all security features including biometric access control and CCTV cameras, network cabling, electrical reticulation, fire suppression, server room design including UPSs and air-conditioning within the server rooms. The client’s requirements included compatibility, future proofing and aesthetic features.

The scope of the project comprised the supply of a high-tech, end-to-end infrastructure solution for the new administration building and a workshop for a group company specialising in prepaid electricity metering. The productivity of the new company was reliant on the completion of the project with a start to finish timeline of two months and a R6,7 million budget. According to Pieter van Wyk, BT-SA Security Project Leader who led the project from start to finish, everything went according to plan with very few hiccups.

“Deadlines, although tight, were meticulously met and as a result the client was left extremely happy with the overall project,” comments Jordaan. “As with many of our larger projects, BT-SA worked alongside a third-party shopfitting contracting company, but our approach is proactive and inclusive, and we work smart to get around potential obstacles. Across the board, BT-SA selected high-tech, state-of-the-art product brands with a national footprint, good technical support and supplier guarantee. This enables BT-SA to provide a solid workmanship and manufacturer guarantee on all installations and paves the way for ongoing maintenance.”

“The initial enquiry was based on word-of-mouth referral from another client. We worked according to strict deadlines and met with the client on a regular basis on- and off-site. All system and design integration happened in-house.”

Reflecting on the completion of the project and the lessons learned, Jordaan is confident that BT-SA met the client’s expectations with regards to design, product and installation, and offered a three-year comprehensive service level agreement (SLA). This SLA is applicable to this project as well as three existing buildings belonging to the group company.

“BT-SA sees this as a long-term relationship and we are currently in the planning stages of the next rollout. What we gained from this project was that if all parties are on the same page with regards to the vision as well as the projected outcome, you can only have success in the end. Transparency, managing expectations and a clear vision of the outcome were definitely the game changing factors in this project,” Jordaan concludes.
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 and users can contact to discuss their integrated security solution requirements.

To list your company here, contact Vivienne at vivienne@technews.co.za or 011 543 5800.

4C Technology
4C Technology is an ‘Electronic Security Technology Integration’ company wholly dedicated to the security needs of medium to large enterprises. We design, supply, install and maintain electronic security systems for customers on a capital and rental basis with contracted service level agreements in place for maintaining systems.

Tel: 0861 42 8324
sales@4c-technology.com
www.4c-technology.com

Honeywell Building Solutions
Honeywell Building Solutions is a leading provider of integrated technology solutions that support innovative ways of working. We develop, install and maintain critical building systems that help keep customer workplaces safe, secure, comfortable and cost-efficient. Global experience across diverse markets positions Honeywell as a technology leader renowned for delivering value.

Tel: +27 (0)11 695 8000,
servicehbsza@honeywell.com
www.honeywell.co.za

Ringmaster Security
Ringmaster Security offers an effective, quality security technology service to the commercial, industrial, retail, education, hospitality and allied industries. We have an intimate understanding of the industry standards applicable to integrated security systems and take pride in the standard of installations, workmanship, neatness, serviceability and levels of customer satisfaction offered.

Tel: +27 (0)11 476 3381
sales@ringmastersecurity.com
www.ringmastersecurity.com

EOH Security and Building Technologies
EOH Security and Building Technologies offer you the “best fit” for all of your facility needs whether it is intrusion protection, fire detection, video surveillance, access control, workforce management, energy control or systems integration – we have the system solutions you need. With a Pan-African footprint and either outright purchase or bespoke leasing offering with maintenance and support options we offer the full turnkey solution.

Tel: +27 (0)11 844 3200
wayne.schneeberger@eoh.com
www.eoh-fss.co.za

JCM Technologies
JCM Technologies focuses on safety and security integration and believes that the proper implementation of security is a must for any business. The company’s solutions not only increase security for business, but through integration its clients can use their infrastructure resources to ensure that they have a cohesive and comprehensive security and safety system.

Tel: 0861 115 359
info@jcmtech.co.za
www.jcmtech.co.za

RR Electronic Security Solutions
RR Electronic Security Solutions was established to provide a complete custom-made electronic solution in the security and surveillance industry. We will be able to advise and implement any sized project, professionally and with as little disruption to business as possible, made up of a highly qualified and experienced team.

Tel: +27 (0)11 021 1071
info@rress.co.za
www.rress.co.za
The ecosystem defines the why for safe cities

By Andrew Seldon.

A safe city leads to a smart city if the project is planned correctly with mutually beneficial goals.

The concept of a safe city is not a new one. The idea has been around for years and many different cities have tried various solutions in the drive to make their cities safer. Some of these efforts have been successful, while others have resulted in failure. The latest addition to the safe city scenario is the smart city, where technology and collaboration offer improved services to residents on top of enhanced safety.


Diender stresses that a safe city is not a matter of technology or having cameras on every street corner. It’s not even a matter of having state-of-the-art control centres, although these eventually form part of the solution. There are many layers to a safe city environment, and each needs to be in place if the next layer is to run effectively.

A safe city project is an enormous undertaking incorporating numerous departments and organisations within the public sector, as well as many in the private sector. The method Huawei starts a project like this with, such as the Kenyan safe city project discussed in this issue, is to begin with discussions with all parties involved to get their buy-in, as well as their commitment to the project. Everyone has an agenda and there needs to be careful discussions that make sure the eventual project is a win-win for all.

The same process needs to happen with partners in the private sector. They, together with the public sector organisations need to cooperate in creating an ecosystem of cooperation in which the ultimate goal is always kept in sight. Diender says that Huawei does not form partnerships in Africa on the traditional basis of offering higher discounts the more you sell, but on the value everyone can deliver and benefits from. The Huawei ecosystem is one of innovation partnerships and not simply technology partnerships.

This ecosystem also includes the residents who will eventually benefit from the safe city (which will lead to a smart city if the project is handled correctly). There is no point in spending millions only to find the residents are not interested or involved.

Why then how and what

Once everyone is on board, the question of why can be addressed: why do we want a safe city? This is where all the stakeholders come to understand the value to be achieved and the necessity of collaboration. Then one reaches the stage where the project can start, or where one can ‘put a stake in the ground’.

In the case of Kenya, the first technological step was to implement a nationwide broadband network. This started with the networks in Nairobi and Mombasa, which will serve as a baseline for the rest of the country. When the whole country is connected, the aggregated knowledge and intelligence from this network will deliver a national ‘smart grid’, which will enable a number of service and safety improvements.

On top of this network, one can build the solutions for various services. One example is surveillance, where cameras installed in Nairobi can be used for safety, traffic, retail needs and so on. This spans different departments, so it is critical that the groundwork is done and everyone works together.

The importance of cooperation can be seen in the following example: suppose someone is attacked in a park. The safe city will then require all the video feeds (as well as other pertinent data) from the scene and the surrounding area to be able to identify the suspect quickly and track their movements after the incident.

This is why a cloud-based solution is also important, since, with a central repository of all data, any authorised people can obtain the information they need to respond and do their jobs. This, again, reinforces the importance of a well-designed intelligent grid.

Integration is key

Of course, the systems on the network and the grid itself are connected to an intelligent control centre (or centres) where centralised services are managed. To ensure all eventualities are catered for, the Huawei platform is able to handle all protocols different solutions require, from radio, to PTT, cellular communications and so on – including social media. This is the ICP of a safe and smart city – an Integrated Communications Platform, also known as an Integrated Collaboration Platform.

While many would question the inclusion of social media in the mix of communication platforms, Diender explains that we are living in a social media world where people react to incidents by first taking and posting a selfie, and then calling the authorities. Aggregating social media posts can provide exceptional intelligence when dealing with an emergency or even in preventing one – such as a riot, for example.

Highlighting the success of this all-inclusive approach, he refers to the Kenyan project as an example where the ability to quickly call up footage and data from before and after an incident is helping to solve crimes. The authorities are now able to solve more crime with less people, and do it faster than ever before.

When taken to the national level, this aggregation of information will have an even greater impact on the lives of citizens. And as citizens are more comfortable in their environment and gain more trust in their authorities, they engage more and are motivated to create their own future. Again a Kenyan example: Nairobi has seen an increase in tourist-related activities and businesses as a result of the safer environment people have since the safe city project started.
Safe then smart
This change, which impacts everyone, from the citizen to the taxes the country collects, is a direct result of the safe city concept evolving naturally into a smart city. As the infrastructure delivers benefits to the security aspect, it expands to add additional value to the broader environment.

It goes without saying, however, that you can't push yesterday's technology to deliver tomorrow's solutions. The safe and smart city requires careful planning and a phased roll-out of different layers, each building on the other. It's worth reiterating that the layers need to work together in an integrated partnership in which everyone wins.

It's no use expecting the police to do everything. They simply don't have the budget or manpower to do so. It is also pointless to expect government to do everything, although both the police and government need to play a major role in the solution. A successful project needs public-private cooperation as it is in the interest of both to succeed.

When engaging in open and mutually beneficial partnerships, the project creates value for tomorrow's needs. It's all about the ecosystem you create to deliver the services and functionality you require.

Value provision
The discussion around a safe and smart city is not a technical one, it is all about value. The value the final system as well as the phases involved in getting to that final state will deliver to each participant in the ecosystem. This value is also what will make the system work. If all the people involved see the value they can obtain from the system, they will participate. If the value is one-sided, some will ignore it and the system as a whole will fail.

The ultimate goal of a smart city and even a smart nation, similar to the Kenyan initiative, requires layers of investment, the acknowledgement of the importance of communications, and the goal or ideal of connected services (such as e-healthcare) meeting the needs of the whole population. So when thinking of implementing a safe city project, the primary question to ask is 'why', defining what value it will deliver. The 'how' comes after you know why it is necessary and the value it will deliver to everyone.

Huawei Safe City Solution can quickly find the smallest needle in the biggest haystack.

Based on industry-leading “Matrix Intelligence” architecture, the Huawei Safe City Solution can automatically analyse vast amounts of data from all available computing resources in a system and quickly find clues through distributive intelligent analysis. This improves analytical efficiency by more than 10 times in helping public security services crack cases.

For more information, please visit e.huawei.com
Or contact us: enterprisebiz@huawei.com

Leading New ICT
Building a Better Connected World
An EPIC first for Cape Town
Cape Town's technology-based public safety programme takes a leap forward.

When facing the challenge of mass urbanisation, cities need to quickly and effectively respond to emergencies and incidents. At the same time, cities need to do more with fewer resources. Metros and municipalities are constantly driving towards becoming smarter, however, before they can be smart, they need to be safe.

The City of Cape Town is well on its way to becoming the safest in the country. When Cape Town’s EPIC (Emergency Policing and Incident Command) programme goes live, it will be the first of its kind in South Africa, providing an integrated public safety initiative that facilitates co-ordinated multi-disciplinary preparation, mitigation, response, and successful timeous resolution of all public safety incidents in the city.

The programme, an initiative in partnership with the City of Cape Town’s Safety and Security Directorate, has been developed over the past two years using the expertise of leading technology solution provider EOH.

EPIC uses SAP technology and spatial real-time mapping to integrate the Directorate’s six emergency and policing services onto one common platform, facilitating collaboration and co-ordination across the multiple agencies. Emma Stavrakis, EOH’s head of public safety and security, says that while many cities have focused on becoming smart, few have drawn the balance between safe cities and smart cities.

Incorporating six primary public safety and security service providers across disaster management, fire and rescue, as well as policing, onto one single integrated technology platform, this programme will revolutionise and dramatically improve the delivery of services in Cape Town’s public safety environment, according to Stavrakis.

"In today’s challenging public safety environment, the ability to understand and respond to the needs of the public is essential. Greater preparedness, improved awareness and effective resource utilisation all lead to enhanced resilience. This is the core of a strategy that will transition the city towards providing an environment that is safer and healthier for everyone," she explains.

According to Cape Town’s Mayoral Committee Member for Safety and Security, JP Smith, the programme will provide the city’s response teams with an integrated and immediate multi-disciplinary response with accurate, up-to-the-minute situational awareness possible across all the city’s public safety services. These include fire and rescue, traffic, metro police, law enforcement, disaster risk management, and the special investigative unit.

"For the public this means quick and efficient response to any emergency they report, efficient dispatching of the resources to the event and proper command and control for the heads of these services," Smith says.

He adds that a unified safety and security system is good news for the City of Cape Town’s vast metropolitan area, which is responsible for a resident population of over 3.8 million people, an annual tourist count of 4.2 million and more than 60 000 businesses.

Smith explains that previously, various departments operated as separate entities, making effective responses difficult, especially in large-scale disaster incidents like the devastating widespread fires experienced in 2012. Technology is now helping the city work smarter, and stay safer. "Now, field officers closest to the incident will always have the correct information and be able to respond efficiently within a few minutes while having access to any information they need," says Smith.

Former paramedic and fire fighter Andrew Mortimer, EOH’s public safety specialist, explains that the EPIC programme is based on the EOH Emergency Suite. This is a single integrated public safety solution that enables all the city’s emergency and policing departments to register and manage their activities.

From the emergency responder to the dispatcher, EPIC assists the department to ensure the most appropriate response is provided to the citizen, while mobile field enablement provides officers in the field with the necessary technology to be effective and remain safe.

Mobility also ensures that officers are able to work smarter, reducing the amount of time in the office. Enhanced business intelligence is provided by the reporting solution, improving decision-making and strategy execution in real time. Investigative case management provides a solution to bring all of the data together and improve accountability in all areas.

Thanks to EPIC, an emergency responder in a centralised call centre can answer emergency calls from citizens dialling 107 from a landline or (021) 480 7700 from a cellphone. In addition, the city’s various safety and security departments and agencies can also log incidents directly on the EPIC system from their automated systems.

The Command Centre then dispatches field officers via a customised mobile app to a mobile phone device that is installed in city safety and security vehicles. Once field officers have dealt with the incident, the status and an incident update are logged onsite via the mobile device.

This includes uploading photo and video information, updating the system in the command centres. Here, all incident details are recorded in the EPIC database for further analysis.

For more information contact EOH, +27 (0)11 607 8346, kedi.bone.sehume@eoh.co.za, www.eoh.co.za.
Leading distributor in the electronic security equipment market
What makes a safe and smart city?

By Neale Strauch, MD, Techsec Security Services (T/A The Lab).

What would it take to make a safe and smart city in South Africa?

As the crime, dishonesty, some lazy and unskilled public servant winds blow over our country, it takes some challenging thought to go down this road again and ask what would make a safe city in South Africa. Having been directly involved in city surveillance in South Africa and other African countries since 1997, completing 29 such systems and handing them over to mostly incompetent service providers, the thought of making our cities ‘smart’ just seems to remain out of reach.

That being said, the question remains, is it possible? Well, yes it could be done, but would need some true and divine effort from politicians, consultants and, of course, service providers who have the political authority to tender.

Let’s firstly have a look at the possibility from a technical or technology point of view. Many of the technology providers have the solutions ready for action installed in their demo rooms. Sales persons are willing to show you what can be done with cameras and detectors overlooking their parking lots, and fabulous interconnectivity to some far away country where the snow covers yet another parking lot, instead of the busy streets outside.

To be fair, most of these providers do not get the opportunity to install these systems in our cities, mostly because of cost – unlike some First World countries where technology demonstrators are paid for. Imagine for a moment if a consultant employed by a city in South Africa would rather go down the route of putting together a budget and paying for a smart city demonstration, instead of inviting the product suppliers with a day’s warning to put up a small-scale system which will be evaluated.

This seems to be common practice, not taking into consideration that these providers are not installers or integrators, thus forcing them to utilise their technical sales and repair staff to do these installations. Such ‘evaluations’ are mostly done haphazardly without any feedback on what could have been achieved, which makes one wonder if the product has not been pre-selected.

A true evaluation?

I would think it is time to set up a system with different products that could be technically and operationally evaluated against a set required operational capability (ROC) matrix and this then be paid for. Now we can start getting to a true smart-city system. Unfortunately, no one will be willing to pay for this and our tendering system would not be able to cater for this.

If we look at the aviation industry, they do not just manufacture an aircraft off the bat. Technology is tested against the ROC, with many exploratory models being built before the final product. An aircraft can land to be serviced and only performs its intended mission for less than 1/3 of its life cycle. Our systems and especially smart-city systems perform this mission 24/7 and costs upwards of R120 million with additional monthly operational and maintenance payments of over R60 million a year.

And when we find the people who are tasked with installing and running these systems have very little technical and operational insight, as we often do, we keep wondering if we can implement a true smart-city system.

Is analytics the answer?

The analytics boom could be ready for smart cities in a few years, but for now only perimeters are protected successfully with this technology. Why then can it not be utilised in the city application? Simply put, Africa is an undisciplined continent and the norm is to break the rules. Analytics needs to identify the exception, like a person walking along the road outside the parking areas. This is the norm in our country and analytics will thus only tell us what we already know, keeping the operator so busy acknowledging this and not doing anything else.

Number plate recognition has its place and can be successfully used to track vehicles

Continued on page 26
SECTOR FOCUS: SAFE/SMART CITY

WiseNet E-AHD Simplicity at its best

SAMSUNG LAUNCHES NEW LOW COST 2MP AHD PRODUCT IN SOUTH AFRICA

Attention Samsung CCTV Dealers & System Integrators

CCTV SI’s and dealers that register with MIA Telecoms before the end of April will receive a free ticket on board the MSC Sinfonia to the Portuguese Islands.

Step 1. Register with MIA Telecoms (Pty) Ltd. michaelr@mia.co.za
Step 2. Place an Order of R 50 000 or more.
Step 3. Receive a free ticket to Portuguese Islands*

*T's & C's Apply

Call us NOW! 011 799 7720
Michaelr@mia.co.za | enquiries@mia.co.za | www.mia.co.za
Continued from page 24

through the city. The footprint or layered approach is needed for this and not hot spotting that has raised its ugly head again over the past few years. Competent designers of smart-city systems are lacking and every time the track and trace is explained, the contradictory response is certainly always the same: “We only need to see the crime hotspots, and when a car that we are looking for enters the city then we can catch them”.

This, of course, hardly ever happens because these criminals just disappear into the concrete jungle and cannot be followed.

Successful smart-city systems should include and manage: traffic management and information systems, traffic light control, overseeing of cash in transit, Wi-Fi for citizens, theft of city assets such as traffic lights and control mechanisms, public address, noise detection, overseeing marches, overseeing tourist groups, vehicle theft, theft out of vehicles and businesses, infrastructure failures, medical emergencies, non removal of street rubbish, SAPS and Metro Police backup and oversight, bylaw policing, help points, floods and many more. All of these city functions can easily be integrated into one smart-city system. Why then is this not really happening?

Integration and intention

Technically this can be done but the approach is lacking. Open a tender document and immediately those in the know can tell you who wrote the specification and put together the bill of quantity. An in-depth survey is never done, thus allowing for interpretation of the bill with items such as power reticulation as a sum amount per position. ‘Allow for 30 m³ can be seen in such bills, but forgetting to mention that some power points can be across the road, which requires civil works.

The approach to a successful smart city should start with the bigger view. Start by defining what the outcome should be, drafting a Required Operational Capability. This should then include all the operational needs, even if some of them are functions and not necessarily technical devices.

This would then lead the way to both sections of the outcome, the technology and the operations.

Survey the city at all its levels

- Layer 1 is the city entry and exit level. Here we identify the entry, to moving through, and the exit routes of the city. Typically, cameras (PTZ domes and static) are placed along these routes. Number plate recognition can be utilised as an aid at this layer.
- Layer 2 is the tracking layer. These are placed along secondary routes and are aimed at tracking vehicles and people along these routes.
- Layer 3 is the trace layer. Generally, these cameras are placed at intersections, using them in all four directions, with a camera at the next intersection one street up. This causes a matrix effect covering the area with a video blanket.

Design the system, based on the information gained above. This, in reality, would mean that schematic diagrams are done, fibre layouts are drafted, power reticulation is determined, lighting levels are documented and an accurate bill of quantity is drawn up. Now have a look at how the other needs can be incorporated into the design. Free Wi-Fi, for instance, could easily be piggybacked onto the system, but this could need more bandwidth and power. So make the alterations to the fibre design, increase the power supply ratings and ensure that there is enough housing space for the transmitters and receivers.

Engage with other governmental departments such as roads, electrical, way leaves, city IT infrastructure, Metro Police and SAPS, just to mention a few. This will then pave the way to successful implementation and possibly save some cost by gathering similar projects under one roof.

The technology choice now becomes the next challenge. Why should this choice be made at this stage?

If the ROC is developed accurately, this becomes the measuring matrix on which the tenderer can be measured. Supplier, other city and other system site visits by the total tender committee would soon show which make or combinations thereof would satisfy the ROC. This should be done before the tender is published or during a pre-qualifying tender process. Why not combine good ideas and good engineering practices from different companies ensuring that the ROC is satisfied?

Unfortunately, it is during this time that corruption can start and this needs to be controlled. Try to appoint a bigger tender committee with more trustworthy members. The bigger the committee, the less are the chances for bribery and corruption.

Implementation, operator selection (not my brother’s father-in-law, brother’s child etc.) and training can now take place, utilising professional selection agencies and installers.

Starting right

We all talk about a set baseline where a portion or a single first point is installed and signed off/redone or even changed completely. Very few companies and clients go through this process that would ensure the baseline is correct, functional and is ticked off against the ROC. A good system is backed by good design, good drawings, engineer change certificates and true, as-built drawings.

In our market, this time is not seen as valuable and even if this is costed into the proposals, it could make the tenderer’s price escalate. This important item on the bill should be allowed for and priced upfront using market-related costs. By doing this, the installer is not under pressure to do this work almost for free and the client has the certainty that the system can, will and does work.

My view is that we can realise one of the first true smart-city systems in the world, but it would take a concerted effort, from all involved, starting with the driver within a city to the consulting engineers, procurement offices, product suppliers, installers, operational service providers, professional selection and training entities with the experience of running such a project and different governmental organisations.

So to answer the question: yes we can.

For more information contact Neale Strauch, Techeac Security Services T/A The Lab, +27 (0)12 654 5985, neale@thelabsa.com, www.thelabsa.com.
SKYHAWK FOR VIGILANT SURVEILLANCE

UP TO 64 BAY 3 YEARS RECOVERY R DATA RECOVERY

*Rescue service available for a premium

pinnacle
Safe city summit in a safe city

The Safe City Africa Summit & Kenya Showcase 2016 in Nairobi, Kenya, demonstrated the value of a safe city within Africa’s safe city.

With the increasing frequency of crime, terrorism and natural disasters, public safety has become a critical issue for governments worldwide. Protecting citizens’ lives and properties means building safe cities that are able to withstand external shocks.

Using new ICT solutions and services, governments can enable a properly connected safe city where visualisation and collaboration are embedded into the city’s infrastructure to maximise public safety. This enables the safe city to become a critical component in smart city development.

New ICT, such as the Internet of Things (IoT), mobile broadband, video cloud and big data, are developing rapidly, and are widely used in areas including integrated monitoring, warning plans, emergency communications, and decision-making support. With safe city solutions, comprehensive perception, emergency command visualisation and effective inter-departmental coordination can be realised, creating a three-dimensional, intelligent public safety system for a city.


The government of Kenya has embraced safe city solutions as a national strategy. Huawei teamed up with Safaricom to implement the first phase of Kenya’s Safe City project, covering the most densely populated cities of Nairobi and Mombasa. Following the completion of the project, these cities have improved their local security and according to the Kenya Police annual report, crime rates from 2014 to 2015 decreased by 46% in areas covered by the safe city project.

Kamal Naim, head of ICT, UN-Habitat (United Nations Human Settlement Programme), stated in his keynote speech that a safer city is grounded on three main pillars of prevention: law enforcement and CJIS reform, social prevention and urban design. An integrated, multi-sectorial approach to improving the liveability of cities and quality of life for all urban residents, predicated on the confidence that good urban governance, planning and management can improve safety.

According to the latest research from IHS Markit, the market scale of public safety equipment is estimated to increase from US$ 13 billion in 2015 to US$ 20 billion in 2020.

Hong-Eng Koh, Huawei’s global chief public safety expert, said in his keynote speech that while intelligent video surveillance, broadband trunked radio and computer-aided dispatch are crucial, they are not enough to create a safe city. There is a need for policing cloud to link up the silos of different public safety agencies for better information sharing and user experience. With the exponential growth of data from traditional policing records, video surveillance, social networks and the Internet of Things, big data analytics are important too. Together these technologies can help in threats prevention, and if not preventable, early detection for faster response and recovery, with the aim of reducing loss of life and property, and bringing justice and normalcy to society.

Partner cooperation to build an ecosystem

At the summit, Huawei displayed its new smart safe city solution, co-developed by Huawei and its partners. The solution consists of the world’s first visualised and converged command system, the industry’s first 4G professional trunking system, cross-region and cross-agency video cloud, and business-driven safe city ICT infrastructure.

Additionally, Safaricom shared its cooperation with Huawei in the development of the Kenya Safe City project. According to a speech from Shaka Kwich, who is the head of the special projects department at Safaricom, the deployments of Huawei’s Safe City solution in Nairobi and Mombasa has drastically improved criminal investigation, cross-agency collaboration, and emergency response efficiency for the national police service. This has resulted in tangible benefits to both the citizens of Kenya, as well as the officers using the solution.

Huawei’s deployment of a new communications network, which links over 1 800 surveillance cameras with 195 bureaux and 7 600 police officers in Nairobi, is of great strategic importance in terms of national and economic security. The National Police Service Commission of Kenya, for example, has a high-speed private broadband network that partly relies on the company’s proprietary wireless enhanced long-term evolution (eLTE) solution.

“The wireless infrastructure links the National Police Service Commission’s command centres with over 1 500 high-definition cameras in downtown Nairobi. Furthermore, it supports more than 200 cameras that are installed at city checkpoints and several wireless devices distributed to officers in the field,” said Frost & Sullivan industry analyst Joanita Roos. “Thus, authorities can conduct panoramic video surveillance of Nairobi’s urban centre, as well as maintain a highly-agile command and dispatch setup that runs on satellite-based global positioning system (GPS) and software-based geographic information system (GIS).”

Additionally, with the video cloud storage platform that Huawei offers, cross-agency video sharing is possible. Through comprehensive security-video linkage, the platform meets multiple service needs, including real-time surveillance, video browsing and evidence collection.

Over and above the video cloud storage platform, Huawei provides sophisticated analytics tools to improve authorities’ ability to identify, classify and match stored video data. The company has also secured its safe city solution against cyber attacks and ensured it is cost-effective.

For more information contact Huawei, +27 (0)11 517 9800, shonisani.mudau@huawei.com, www.huawei.com/enterprise.
WORLD-CLASS AUTOMATIC NUMBER PLATE RECOGNITION (ANPR) TECHNOLOGY

ANPR
(Automatic Number Plate Recognition)

KEY BENEFITS:
- Ensure maximum security
- Identify stolen vehicles
- Deny unauthorised access
- Allow access to employees and tenants
- Create blacklists and whitelists
- View events from specific timeframes
- Generate reports

Feature Rich Video Management Software
info@cathexisvideo.com | www.cathexisvideo.com
Elements of a safe city

By Andrew Seldon.

The components of a safe city are demanding, but the benefits worthwhile.

The idea of a smart city might have been laughable in South Africa in the very recent past. The concept of a safe city even more so, but things are changing. There are numerous technologies used in a safe/smart city, security related and otherwise, but the ideal of a safe and smart city starts with people, public/private cooperation, extensive planning, and the will and cooperation to make it happen.

Hi-Tech Security Solutions asked Francois Stander, responsible for research and resource development at the Tshwane Metro Police Department, for his thoughts on some of the issues critical to a safe city, which is the starting point for a smart city – we refer to both as a safe city in this article.

The reality of a safe city is that it is extremely rare, read impossible, to work on a greenfields project where you get free reign in the planning and design. Existing cities already have infrastructure of some kind and some form of security operations, even if it is weak and ineffective.

However, you must start somewhere and Stander says, “At its core, a safe city project must address and plan for four key ingredients as an integrated concept from the start, even if all four are not contained in the same phase of implementation.”

Stander expands on these four factors below.

The four key ingredients

1. Centralised Command Centre (CCC)
   The city must bring all emergency, security and key service delivery departments together in one integrated command centre. This allows the city to have one coordinated snapshot view of all ongoing situations/problems and ensures a coordinated response from all departments. This is especially important during large events, natural disasters or even just incidents that involve more than one department, like motor vehicle accidents that can involve Metro Police, emergency services, electricity, roads, storm water etc.

2. Dedicated fibre and broadband communication network
   The ability for all emergency and security services to communicate is fundamental to any safe city. The platform used for communication must allow voice and data transfer at high speeds to accommodate live multimedia data and must run on a dedicated and secure backbone fibre and radio high-site network. The strategic importance of this communication network requires that it not be affected by public use and load factors, and can therefore not run on a commercial backbone LTE or other networks.

3. Macro surveillance network (CCTV)
   A citywide CCTV network, feeding directly into the CCC is essential to enable monitoring of public spaces, incidents, people, roads and infrastructure. Live video of incidents allows rapid response from the CCC with the appropriate resources, greatly reducing response times.

   The CCTV network must be expanded to include commercial networks at retail centres, filling stations, neighbourhood watches etc. The aim is to bring together the information from all public CCTV cameras through the linking of modern IP-based camera networks and their respective control rooms to the CCC. This will naturally exclude private cameras.

4. Integrated information management system
   No safe city project can function without a significant ICT component and indeed must have at its foundation a comprehensive and integrated software system that manages all processes, resources and integration.

   This integrated management system must be designed to manage the following:
   • Workforce management.
   • CCC call taking and dispatch.
   • Mobile application portal between the public and the CCC.
   • Internal mobile application portal.
   • Electronic law enforcement (handheld, ANPR, etc.).
   • Crime and accident analysis, analytics, AI, reporting, statistics, etc.

   • Integration of systems and information with other agencies (SAPS, other cities, etc.)

The subtle thorn of cooperation

Having all the bits and pieces in place is only one of the steps in a successful safe city project, however. Another critical component, some would say the most important one, is to obtain the buy-in of all parties involved. It’s easy to get the nod from various departments who will gladly agree to an integrated project, but when it comes down to actually working together and integrating people, processes and technology, things can get sticky.

As noted above, it’s not only the public sector that has to be part of the safe city. To be truly successful, the project needs the full support of private organisations as well. A mall, for example, may already have a host of cameras and other security operations in place that can provide invaluable information to the CCC.

These types of partnerships must also be forged on a basis of trust and cooperation.

Stander says there are many opportunities for the public and private sector to benefit from a safe city project. A few of these include:
   • An integrated control centre clusters all essential services together and ensures that there is one access point into the services of the city. The response is coordinated and would ensure that departments can directly collaborate to address multi-departmental complaints.

The CCC will further aim to link control rooms from private sector security services, CPFs and neighbourhood watches directly to the CCC and these companies will then have the benefit of shared crime information and resources when responding to incidents.

   • Linking CCTV camera networks directly to the CCC allows businesses to have another layer of response to incidents over and above their own control centres. This also allows Metro Police to get live video of an ongoing incident while they are on route to the scene.
especially crucial during violent incidents like ATM bombings and mall robberies.

• With a full safe city concept in place, the Metro Police will function more effectively and efficiently across the board and this will allow amplified cooperation and interaction with all public and private role players. Systems will be available to streamline interaction with the city as well as to automate processes, like getting accident reports, applying for events, paying or enquiring about fines, etc.

• A citywide communication network ensures that every Metro Police member is always connected to the CCC and the rest of the department. This means that when one member responds to an incident, the whole department is instantly available to assist and that member has instant access to all the relevant information they need to assist someone.

• The inevitable reduction in crime that will come from a comprehensive safe city project will benefit every citizen of the city and will boost economic growth.

**Essential components**

There are, of course, many technical aspects to a complete safe city project, however, there is one key area that Stander says is essential, a citywide fibre network. "If I had to pick one requirement of a safe city project," he notes, "it would be that all components must be able to communicate with each other over high speed and dedicated infrastructure."

Some other important solutions for a safe city, according to Stander are:

• A modern mobile application that can serve as a portal for the public to access the CCC. It should be able to handle reporting of incidents as well as give feedback on actions taken. This solution scales much better than only having a telephone public portal and complaints are received and acted upon much more accurately and reliably using geo-tagging and other mobile phone features. Mobile applications for internal systems and processes will also ensure much more effective workflow.

• Technologies like automated number plate recognition (ANPR), video analytics on CCTV cameras and crime information analysis tools can all greatly enhance the effectiveness of a safe city project.

Stander describes ANPR as one of the most successful applications of new technology of late, especially when linked to centralised databases (eNatis, stolen vehicles, etc.). A network of these cameras across a city can quickly flag wanted vehicles and suspect vehicles can be circulated to the system in seconds.

"This makes it virtually impossible for a wanted number plate to drive anywhere in the city without being flagged by the system. Think of robbers that drive around looking for targets. They can be flagged by neighbourhood watches or CPFs within minutes and the vehicle will in most cases be flagged and intercepted before they find their first victim."

• Another exciting development is the advent of video analytics that can monitor thousands of live CCTV video feeds. "I have seen demonstrations where the police can search through CCTV footage for a male with a red t-shirt and the system will return all video footage of males with red t-shirts (to an impressive degree of accuracy). This technology has already yielded very positive results in the tracking of suspected bombers in Europe and the USA."

• From a systems and information point of view, the ability to integrate all relevant crime information from all agencies in the country will ensure that members on patrol do not drive past a stolen vehicle or give a traffic fine to a wanted murderer just because they did not have access to all the information.

**The people problem, or solution**

Despite the advances of technology and those people who are touting artificial intelligence as the answer to everything, a safe city has and will, depend on the performance of the people working for the city and those receiving services and feeding information to the CCC. Making sure your people, staff and public are geared to operate effectively is critical to the success of the project. Not only is training required before the project rolls out, but continually to ensure the best service is delivered for the long term.

"Change management remains a problem with any new system or technology that is introduced," says Stander. "I believe that this should be planned for from the inception phase of the project and sufficient resources must be made available to handhold end users during the initial deployment of the project. I have found that if you have on-site personnel that can assist during the early period, it eliminates a lot of the resistance and ensures that misconceptions and misinformation do not take hold.

"This goes hand-in-hand with a comprehensive training programme and it is essential that users do not just show up to a new system one day. Every user and supervisor must be trained and prepared for the launch. The control of information should as far as possible be designed into the electronic systems that manage these processes. There should be electronic systems and processes that have all business rules included and that should greatly reduce human errors."

**Miracles require hard work**

Despite the potential for safe cities, which extends from security through to economic development, why do they seem to be so hard to find in South Africa?

One obvious answer is the cost. These are enormous projects that will consume tens, or more likely hundreds of millions of rand to roll out properly. This is money that has to be found and spent before any of the benefits can be realised.

Stander believes the hardest part in getting a safe city project rolling is moving the city and the Metro Police to commit to implementing the project. "It involves convincing politicians and executives to identify the benefits and positive impact of such a project," he says. "The scope and capital investment required will make most financial departments recoil at the very thought of it."

He says it is therefore important to clearly communicate the benefits and long-term savings to the decision makers. Multi-year phased implementation, public-private partnerships, grant funding, etc. should all be explored and presented. If properly packaged, presented and explained, it is not hard for a city to see that the positive impact will far outweigh the cost of implementation.

"The actual implementation of the project would be a massive undertaking and I believe there must be one overall project team that can ensure coordination of specifications and requirements across different aspects and phases of implementation. It would be easy to end up with systems that do not support integration or expansion with the rest of the project."

A safe city is a dream that delivers exceptional benefits if done right. The catch is, it is not easy to get it right in the best of circumstances, and even harder when politics and personal fiefdoms, as well as the threat of losing control loom large.

Hi-Tech Security Solutions would like to thank Francois Stander for his efforts in providing input for this article.
Eyes open in the bus

Rosario, Argentina has undertaken a citizen-focused security project to implement surveillance cameras on public buses.

Instances of crimes and violence (especially on city buses or at bus stations) motivated the Argentine city of Rosario to improve safety and security measures on the Urban Transportation System – or TUP as it is known locally.

Increasing the police presence to include an officer on each bus was both cost-prohibitive as well as uncomfortable for some TUP passengers. The final project proposal was based on best practices from other similar municipalities and involved an increased reliance on security cameras in each TUP bus.

The public tender was opened at the end of 2015, with eight companies presenting proposals. Ultimately, Crayon Web was awarded the contract to implement obvious but unobtrusive cameras throughout the TUP bus system.

How does it work?
The project began with 50 buses outfitted with three security cameras. One camera sits over the driver’s seat and focuses on recording passengers entering and exiting the bus. The second camera perches near the driver’s seat and faces the rear of the bus. The third camera is mounted above the last row of seats, aiming toward the front of the bus. All of the cameras are capable of recording audio as well as video. The cameras are connected to an NVR equipped to record 45 days of footage.

The camera footage is accessed and viewed remotely from one of seven terminals. Two of these terminals are in the 911 emergency dispatch centre; two additional terminals are at the mobility monitoring centre; and each of the three public transit companies – Semtur, La Mixta and Rosario Bus – operate one terminal each. Security camera footage is immediately reviewed by an operator at one of the seven terminals and first responders are dispatched when necessary.

At the time of writing, 300 Mobile IPC DS-2CD6510D cameras, 150 Mobile IPC DS-2CD6520D-10 cameras, and 150 NVR DSM 7508 HNI/GW/WI network video recorders have been installed.

Hikvision’s local distributor, Security One, played a crucial role in this TUP project. Security One provided the technical and training personnel to assist in presenting the proof of concept demonstration to Rosario municipal government, as well as configuring and installing the 3G and 4G networks on each of the buses. The Security One team even arranged for Crayon Web staff to travel to the Hikvision manufacturing facility in China to integrate their software with the custom-built video surveillance system.

Support for municipal security
The first phase of the project involved installing 150 cameras and 30 NVR units throughout a test fleet of 50 buses. A 10 MG asymmetric and dedicated network was installed in the mobility monitoring centre. The total cost for the first phase was approximately US$1.5 million.

Phase two is scheduled to include 300 additional buses. This will require 900 cameras and 300 network video recorders.

This project works in conjunction with fixed location surveillance cameras which have been in limited use throughout Rosario for several years. As both systems integrate and expand, Rosario will become the example for every Latin American city facing the challenge to curb urban crime.

The monitoring terminals rely on the available 3G networks. This large-scale network allows for high-quality audio and visual streaming from the buses to the seven monitoring stations. Crayon Web manages all onsite technical support, including preventative maintenance for individual cameras, monitoring terminals, and any new components. The Hikvision/Security One/Crayon Web alliance enabled Rosario to adopt the North American ‘Eyes of the City’ concept which will allow city officials to monitor traffic situations, environmental concerns, and assist in law enforcement duties – all with the aim of improving the quality of life of the community.

During testing of the TUP system, which included the activation of bus-driver panic buttons and dispatching police, the public was able to see how Rosario is beginning to take the lead in public safety. Similar systems are already in use in Thailand, Istanbul, and Dubai. More than 1.5 million people in Rosario consider this new system to be a positive step toward solving crime problems plaguing Latin American cities.

For more information contact Hikvision South Africa, Evan Liu, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com.
Radwin announced that the Windhoek Police Department in Namibia built a state-of-the-art wireless video surveillance network using Radwin’s wireless broadband access solutions.

Radwin’s Point-to-Multipoint and Point-to-Point systems were installed in dozens of crime hot-spots throughout the city. The systems transmit high-quality video from the cameras directly to police headquarters, enabling on-the-spot detection and response to events. Rampoint Communications, a leading turnkey solutions provider, was responsible for project design and implementation.

Cillie Auala, spokesperson for the Windhoek City Police said, “Initially we used a Wi-Fi-based solution for CCTV transmission, but decided to upgrade our legacy network because it did not meet our requirements for high-capacity transmission and our safety and performance standards. Now that we are using Radwin’s systems, we’re getting highest video transmission quality with zero video pixilation and low jitter – which is vital for our mission-critical operations.”

Andre Delport, MD, Rampoint Communications, added, “Namibia’s vision is to be the safest African country by 2020. To deliver on this vision, we recommended Radwin’s Point-to-Multipoint systems which deliver dedicated bandwidth per camera site with 90% uplink traffic and mega-capacity of up to 750 Mbps, as well as Radwin’s Point-to-Point systems for backhaul. From our extensive experience, Radwin’s solutions operate in the toughest urban environments, overcoming interference and line-of-sight obstacles to deliver superior video performance.”

Peter Turvey, Radwin GM Africa said, “With our wireless broadband solutions, the city’s police forces and first responders can monitor and address unfolding situations in real-time and use high-definition video surveillance footage, enhancing the safety and security of citizens in Windhoek.”

For more information contact Radwin,
+27 (0)74 114 2805, nick_ehrke@radwin.com.
South African smart cities

South Africa’s safe and smart cities are starting to take shape, albeit slowly.

When one thinks of smart cities, one might be forgiven for overlooking Africa, but not for much longer as the technology is in play and expanding rapidly. South Africa in particular offers an increasing focus on developing smart cities to the extent that the South African Local Government Association defined the term to coordinate the development throughout the country.

Defined as a city which ‘uses digital technologies to enhance performance and well-being, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens’ they have focused on the smart sectors of transport, energy, healthcare, water and waste.

With the country’s population rapidly urbanising and the needs for each city being different, it’s to be expected that each would make use of technology in different ways to suit their needs. For example, Cape Town has set up a digital integrated transportation system while Johannesburg offers residents the ability to digitally report infrastructure faults. In 2005, Pretoria partnered with Oulu (Finland) to compare best practices, resulting in an unprecedented roll out of free Wi-Fi to over 3 million people.

The roll out of free Wi-Fi is part of Project Isizwe, a drive to disseminate Internet throughout the country. Much of the infrastructure, from Wi-Fi on buses to powering South Africa’s largest wireless ISP is issued by Radwin.

Unfortunately the country is still held back by the lack of accessible cheap mobile data. Research ICT Africa has reported the average cost per gigabyte in South Africa as US$ 5.30, which is marginally higher than economic competitor Nigeria ($4.90) and significantly higher than Egypt ($2.80). South Africa has also seen marginal, yet consistent, drop in position in the International Telecommunications Union's ICT Development Index where she currently sits in the 88th place owing to improving slower than the rest of the world. Despite this, South Africa places third overall in Africa.

With just over half of the country’s 55 million population connected to the Internet (primarily through mobile devices), it’s easy to see why the high costs are barriers to connecting the other half of the country and, by extension, limiting the development of smart cities.

Steve Pinto, managing director of New Reality, South Africa’s forerunner in advanced coding for augmented and virtual reality devices, says the country is feeling the pinch of the limitations. He cites the lack of broader infrastructure as well as the focus on small projects as opposed to ones on a national scale as the primary stumbling blocks.

Pinto claims that “smart cities are vital to humanity in today’s world and that when we have them, people’s lives change for the better but we need to desperately meet the increasing demand on infrastructure by improving supply to make these cities happen.”

South Africa seems to have the building blocks for developing complete smart cities, from political will to developers ready to code. Where it’s lacking is in the low infrastructure and costs of connectivity. With one of the highest Gini coefficients in the world, it’s not surprising to see that the country is struggling to balance the data market with the private sector, rather opting to cater for the have-nots. That being said, the development of free Wi-Fi in certain metropolitan areas should not be scoffed at and is certainly a step in the right direction.

While a fully-fledged smart city is not on the cards for the tip of Africa tomorrow, it’s certainly on the cards for the near future. Chinese firm, Shanghai Zendai, has dedicated over $8 billion into building a 35 000 house-smart city over 1600 hectares just east of Johannesburg.

For more information contact Radwin, +27 (0)74 114 2805, nick_ehrke@radwin.com.

Western Cape Improvement Districts get timely software and security boost

Local software improves security, data collection and management.

Residents living and working in Cape Town’s progressive City Improvement Districts (CIDs) have been boosted by the introduction of new software that promises to improve security and overall maintenance services.

CIDs are demarcated management zones or special rates areas (SRA) approved by the City of Cape Town, where the majority of property owners (business and residential) contribute a nominal additional fee for top-up value-add services like security patrols, cleansing services and urban maintenance.

The majority of Cape Town’s major CIDs – namely Groote Schuur, Claremont, Wynberg, Voortrekker Road, Observatory and Woodstock – are now managed by global protective services company Securitas, using locally-developed incident management software called Incident Desk from Cape Town-based South African software company Solution House.

According to Securitas South Africa business
development director, Jeremy Horner, larger CID's average 2000 to 3000 incident reports a month, so the company needed a way to consolidate its incident reports and integrate multiple monitoring and reporting systems both within and between the various CIDs on its books.

“We deliver these services in support of – and in collaboration with – city-funded resources like the South African Police and Metro Police, so we’re complementing rather than replacing their functions in these areas,” says Horner. “To do so effectively, however, requires substantial logistical resources, including powerful software tools like Incident Desk that help us record, manage and report on all the data we need to manage in each CID.”

Horner says that while CIDs have become one of the major success factors in the upliftment of Western Cape communities, they also generate enormous amounts of data and deploy many different systems – both manual and electronic.

“Effective management means staying ahead of the curve when it comes to knowing what your customers need from you, be it from a security perspective or any other service they pay to receive,” he says. “One of the main challenges we face from a management perspective is breaking down the silos of information not only within a CID, but also between CIDs, because issues that affect one CID often spill over into an adjacent district. This is where Incident Desk, with its consolidated view, smartphone app and ability to process information from different systems and management areas in real time, comes into its own.”

Solution House director, Tiaan Janse van Rensburg says public safety management is a good example because urban management companies often have to deal with many inter-related challenges such as social services, maintenance and by-laws.

“Using a single system that allows us to aggregate incident reports from these various sources and quickly see where, when and how often certain crimes take place in demarcated areas within a CID, allows us to identify trends and hotspots and predict when and where we’re likely to see them re-occur.”

“While Incident Desk consolidates information from any number of CIDs, it is actually part of a larger national urban management and public safety solution which centralises information for the whole of South Africa. This ability to predict and prevent crime makes it possible for CIDs to become far more proactive in their service delivery, which ultimately sets them apart from urban management models that are predominantly reactive.”

Incident Desk is a universal incident mapping and management platform that provides estate and security managers with real-time incident alerts, and gives them the ability to record and report live incidents with a smartphone application.

For more information contact Tiaan Janse van Rensburg, Solution House, +27 (0)82 565 8081, tiaan@solutionhouse.co.za.

SECTOR FOCUS: SAFE/SMART CITY

UNLOCK CCTV’S FULL POTENTIAL

Mass provides customised electronic security solutions THAT WORK TO THEIR FULL CAPACITY!

CALL 012 142 0000 NOW!
www.mass-solutions.co.za
Are the rights of some more equal than the rights of others?

By Chris Cobb, Kifaru Management Services.

1976 reloaded. . . “For as long as the system denies access to poor students we will render it dysfunctional.”

One striking feature of last year’s student protests is that they were organised beyond party and ideological divides, and the effective use of social media played a huge role in its effective mobilisation. It was this fact, more than any other, that brought thousands of students and their supporters onto the streets at Parliament, Cosatu House, the Union Buildings and marching on Cape Town International Airport. It was also this multi-class and multi-racial alliance that shook up the state and prompted it to be partially responsive to the students’ demands.

There is no doubt that the violence involved in many protests was in part facilitated by strands of the movement that deliberately adopted a strategy of violence. In part, this was prompted by interpretations of the writings of Frantz Fanon who was seen as an advocate of revolutionary violence. However, it is important to state that the vast majority of student protestors respected the boundaries of peaceful protest.

The flashpoints

The writing was on the wall as far back as Tuesday 10 January 2010 when UJ highlighted symptoms of how SA is struggling to meet demand for education among the poor.

• 20 people injured as thousands of students clamour for last-minute places.
• A woman crushed to death in a stampede.
• More than 180 000 prospective students turned away from the country’s top nine universities (UJ 74 000, KZN 61 500, Wits 30 000, FS 13 000, PTA 35 000, Tshwane 30 000, NMU 31 142, and UCT 26 000).
• 1st year places available (UJ 11 000, KwaZulu-Natal 9000, Wits 5500, FS 4000, PTA 13 000, Tshwane 8000, NMU 5472, and UCT 4000).

The violent student protests in South Africa began in the north at Tshwane University of Technology early in 2015 when students were prevented from registering because of outstanding fee debts. This was exacerbated by the inability of the state loan and bursary agency – the National Student Financial Aid Scheme (NSFAS) – to meet its commitments.

Confrontations spread to other campuses, taking different forms. Students at three universities in the south were next to act.

• At the University of Cape Town, students took issue with the legacy of colonialism, symbolised by the memorial to Cecil John Rhodes.
• Students at Stellenbosch distributed a powerfully evocative film – Luister (Listen) – that documented black students’ daily experiences of racism and discrimination.
• Students at the University of the Western Cape protested against levels of debt that would prevent them from graduating.

Dissent crystallised into a national movement in October 2015, when universities began to announce fee increases in excess of 10% for the 2016 academic year. The government, initially dismissive, was forced to impose a freeze on fee increases and find emergency funding to compensate universities for their loss of revenue.

Collectively, this became the largest student social movement since the dawn of South Africa’s democracy in 1994. It shook up the state, changed the systematic parameters, and began the process of transforming our higher education sector.

Yet, this united student movement fractured soon after President Zuma announced the zero percent fee increase for 2016. This was partially due to the natural process of the mainstream of the student body withdrawing and concentrating on completing the academic year after their immediate collective demand had been achieved.

Transformation moved to the heart of the national discourse through two sets of events: the #RhodesMustFall and #FeesMustFall movements, emanating from two major challenges facing higher education: alienation and access.

The uprising has specific roots in apartheid and colonialism. But issues of race, identity, fees and unemployment are provoking unrest across the world where the propensity of violence manifested itself at its most extreme level as the protests wore on.

During the past two years, violence at South Africa’s universities has escalated:

• Malicious damage to statues, artworks and buildings.
• Intentional provoked confrontations’ with campus security, staff and police.
• Preventing the distribution of food for students in residences.
• Attacks and assault with deadly weapons including knives.
• Burning of buildings and other assets.
• Sabotaging of critical infrastructure.
• Disruption of the academic programme.
• Evictions by means of intimidation of staff and students from lecture venues, offices, residences etc.
• Intimidation.
• Taking staff members as hostages.
• Burning and damaging private, outsourced vehicles and transport.
• Defacing property by means of graffiti, human faeces.
• Looting of shops, food outlets vendor machines.
• Theft of monies from POS, safes, vendor machines etc.
• Unlawful squatting in residences.
• Theft of university assets.
• Brutal clashes between different student factions.

Chris Cobb, Kifaru Management Services.
Challenges

Violence, where life safety was at risk, often compelled the institutions to call on the state to respond with non-lethal force in order to protect public property which resulted in creating a militarised atmosphere that worked against the immediate interests of the protestors and the legitimacy of the protests itself. Police were only called in once protestors had already resorted to arson and violence as the law states that a crime has to be committed and lodged with the SAP before they can respond.

Both open (part of the community) and closed universities are faced with a multitude of serious issues when attempting to address the security challenges around violent, protesting students. Six key activities typically need to be undertaken when dealing with student protests:

- Controlling entry into a venue or event.
- Monitoring and communicating on crowd and individual behaviour.
- Dealing with potentially aggressive, abusive or violent behaviour.
- Physically managing aggressive, abusive or violent behaviour.
- Administering and coordinating ‘first response’ first aid or critical care.
- Coordinating emergency evacuation of a venue or event.

But that’s not all. There are also a myriad of other considerations:

- Effective and agreed upon, predefined Rules of Engagement to address the listed risks above ranging from students attempting to breach venues to disrupt classes and exams, to preventing acts of arson etc.
- Rules of Engagement and a tiered crisis alert escalation guidelines need to be developed for:
  - Command, control and incident management.
  - Reporting levels of escalation.
  - Assessing points intervention and level of intervention response.
  - Identification of security lines and containment areas in crowd performance.
- Establishment of an effective Core Crisis Management Team and communication platforms to all – core crisis team, SAP POP, media, alumni, donors, council members, students, government, other external agencies (fire, traffic etc), academics, staff, other universities (legal teams etc.).
- Understanding crowd behaviour and crowd management in which campus protection services/SAP POP personnel focus on is the end phase, namely the dispersal.

In conclusion

Major concern is that protestors are so focused on their rights that they had forgotten their obligation to respect the rights of others. And while it is the goal of peaceful protest to create inconvenience and disruption, it is definitely illegitimate to violate the rights of others on such a wide scale.

So the question at large is how does one enable the evolution of a social movement for the legitimate struggle for affordable higher education, without allowing it to undermine and weaken the various institutional commitments to being a free and safe space for ideas, while balancing the competing interests and rights of a variety of stakeholders, including those within the student community who were intent on completing their academic year?

The message: avoid confrontation. It is a game you don’t want to play unless you have to:

- Crowd situations are highly unpredictable.
- One thing is certain, confrontation in most instances will likely cause crowd resistance – the ‘closed loop, negative feedback’ model.

For more information, contact Christopher Cobb, Kifaru Management Services,
+27 (0)72 596 2621,
chris@kifarumanagement.co.za.
Education must not fall

By Andrew Seldon.

Fees must fall, but education can’t be allowed to fall in South Africa.

Last year South Africa saw several demonstrations (or riots, depending on who you ask) at our leading universities under the banner of ‘Fees Must Fall.’ While many demonstrations went off without violence, it seems there were some elements seemingly determined to turn a legitimate protest into a battle with the police, administrators and even other students trying to continue their studies.

Commenting on the Fees Must Fall campaign is beyond the scope of Hi-Tech Security Solutions, but some of our readers were caught in the middle as they tried to retain a semblance of order at the universities they work for, allowing those students focused on their studies and academic staff committed to their students to continue their work unhindered.

To obtain a clearer understanding of how the various security and risk operatives at our universities handled the crisis, we asked a number of them to expound on their experiences and the actions they took – as well as lessons learned – while they tried to look after our higher education institutions.

Hi-Tech Security Solutions: What have educational institutions learned when it comes to dealing with popular demonstrations?

Viljoen van der Walt: Like various other university campuses in the country, Stellenbosch University, for the past two years, was not exempt from attempts to destabilise the campus and its academic programme, but to a large extent we were able to complete the academic year successfully. In this regard, probably the most important lessons from a security point of view was to be informed, to have contingency plans in place to deal with different security challenges and to keep the various affected target groups up to date on the situation on campus.

One should, furthermore, take into account that the national political situation has a direct influence on what is happening at campus level. Very often it was not about the demands in itself – often protestors kept on protesting even when their demands were met. Attempts to reconcile and resolve issues were met with making new demands, in most cases deliberately out of reach.

Protest leaders followed a methodology in which they would start by taking control of a facility – with the aim of confronting executive management from that vantage point – and then to create ‘conflict’ situations in an effort to close down the institution. Security services are the barrier to overcome the drive to get to management.

Moreover, disinformation and false accusations were used as strategy to discredit senior management and the security division.

Derek Huebsch: The importance of information and intelligence in advance and the sharing thereof has made it possible to better engage and manage situations of this nature, which have become ‘the new normal.’ This includes the importance of engaging with and keeping all other stakeholders, such as staff, parents and non-participating students informed, to dispel the negative perceptions, rumours and disinformation that is so easily circulated by way of social media or word of mouth.

Noko Masalesa: The availability of the executive management, their direct involvement in the safety and security plans of the university, and their ability to engage with the different stakeholders during a protest are crucial during a protest action.

Hi-Tech Security Solutions: Were your security teams ready to deal with the unexpected turn of events?

Continued on page 40
Continued from page 38

**Van der Walt:** There were some surprises. On a few occasions, protestors were able to enter buildings and disrupt academic activities. But as we became more informed on strategies and tactics used, it was possible to prevent the disruption of academic activities most of the time. One should keep in mind that the university acknowledges the right of staff and students to take part in protest action as long as this does not pose risks to the safety of staff and students, or to university property, and provided there is no breach of the rights of students to study or to write their exams.

**Huebbsch:** Being caught in the midst of the student protest action whilst going through an in-sourcing process of support staff employees was extremely difficult as it added to our problem. Some employees felt and were regularly reminded by student protestors that they had fought to get them in-sourced so they were expected to look the other way and not report or get in the way of student protest action.

This led to a large amount of the uncertainty with respect to safety and security amongst non-participating parties. It also led to additional expenditure in respect of having to outsource and obtain ad hoc security services for the duration of the period between mid-September and 21st December 2016 when the last exams were written.

One of our immediate needs is that of conducting sound skills assessment tests and training of the recently in-sourced officers and most likely having to again obtain ad hoc services to provide the necessary safety and security during the initial stages of the 2017 academic year for late exams, re-exams and registration periods.

**Mmapulana:** Yes, we have a written security plan where we documented plans of action in case of wildcat strikes for both employees and students. We are always ready as we experienced student protests from 2015. We improved many security measures that I cannot mention here.

**Naidu:** Yes we were. We had to bring in additional security resources as the aim was to complete the 2016 academic year, which was achieved. During the 2016 examinations, we had no disruptions at the various internal venues used. The difficulty that we faced here was dealing with very small numbers of protestors, those working in groups of three, four and five. We lost only one building during the demonstrating and it was a sports clubhouse. There were attempts to disrupt some of the exam venues, but this was avoided. The common damage was broken windows.

**Masalesa:** Yes, my team was always ready because we met every morning with our SAPS and Riot Control Service providers to discuss mitigation measures. Before we went off duty every afternoon, we also went through lessons learned for the day and made the necessary adjustments.

Continuous improvement is part of our department’s management philosophy. We continuously look for areas requiring enhancement and focus on those. We do not say everything is working well and start relaxing.

**Hi-Tech Security Solutions: How important is the ability to communicate with all parties effectively in a situation like this? What did you do to keep everybody informed?**

**Van der Walt:** Communication is key. It is essential to counter disinformation and to keep staff and students informed and to continuously emphasise the continuation of the academic project. Social media is an important tool to provide information, but can be a digital ‘battlefield’ during protest action. Often, well intended messages by the university were met with disinformation, so social media has a positive and a negative side to it. It was important to the university to have a website that was updated on a regular basis – social media was used to direct staff and students to the website. Regular communiques to staff, students, alumni, donors and parents also proved to be very valuable.

**WhatsApp groups with different groupings of staff, security and safety teams proved to be the best, fastest and most reliable source of internal communication between the main role-players.**

**Huebbsch:** Communication, communication and communication is of utmost importance, without it the majority of stakeholders (non-participants) are left in the dark. Our worst enemy is also our best ally, that being social media, and unless it is used and relevant information circulated by the university ASAP, the risk exists of disinformation and negative remarks and rumours being posted. This would leave the university with the impossible task of trying to save face. Being informed makes for educated decisions and awareness on the part of all affected and must not be left to risk. As CAMPROSA President, I initiated a communication link between institutions with the intent of sharing information and experiences during the past year’s protest action. I believe this assisted us all in better understanding and collaborating in our efforts to deal with the new and difficult challenges brought about by the situation.

**Mmapulana:** It is very important to communicate with all stakeholders during protests, especially parents. We have an SMS system that we use to communicate with parents, students and employees. We also use social media and notice boards.

**Naidu:** Communication is vital; however the problem is that security information on planning can be leaked. Therefore, certain information had to be furnished at the last minute to academics and students. I ran the JOC from the security office and coordinated the ground security at the various areas of the campus.

**Masalesa:** The ability to communicate effectively with all stakeholders is critical. In our case, we are very fortunate because we have a hands-on Head of Communication and Dean of Student Affairs.

Daily updates were provided to the Head of Communication and Brand Management. This included, for instance, the number of arrests (if there were any), as well as any disruptions reported and/or observed etc. This ensured that accurate information was communicated to the media. The agreement between us was that any article relating to protests must first be checked by me before it could be sent out.

Since we have three campuses, various additional communication options, such as push-talk radios are being investigated to ensure that there is proper command and control during protests and any other emergency situations.
**Hi-Tech Security Solutions**: In hindsight, how do you think it is best to include everyone on campus in your security plans?

**Van der Walt**: All university buildings must have an effective and well-functioning safety committee and staff must take part in, for example, evacuation drills. Furthermore, academic staff are also informed as to what to do during class disruptions. On a security level, there is a communication strategy, but this is, of course, on a ‘need to know’ basis for obvious reasons. In 2016 we were, to a large extent, able to develop and maintain target group focused communication. It was important for us to balance disinformation with the facts, even in the face of intimidation. It should be stressed that the overwhelming majority of students do not want the destabilisation of the academic project.

**Huebsch**: Using all available means of communication is important, not only posting it on a safety and security website, it is also relevant to post visible and effective signage throughout campuses, buildings and facilities. What is also important is that such information is easy to understand and offers the assurance that all possible methods of ensuring the safety and security, and sound evacuation of people has been thought of. Early identification and prevention of potential risk or exposure to risk must be an effective part of the process. Decision making in respect of when and what to do should the situation become risky or pose any potential threat should be streamlined, and the use of a small yet representative emergency team to exchange ideas worked well for us.

**Mmapulana**: We have a good relationship with student leaders and we engage with them.

**Naidu**: Creating a business continuity processes and a crisis management plan. All relevant stakeholders must play a part in ensuring that there is completion of the academic year, working with designated persons to perform coordinating roles. This can be achieved via effective team work – meaning all departments, be that academic or support, work together.

**Masalesa**: We have established emergency and crisis management committees at our three campuses which have representatives from each department and faculty. Every department and faculty has appointed a safety and security champion who works closely with the Protection Services department. The (champions’) responsibilities include, among others, to ensure that their buildings have emergency management plans and clear protocols with critical contact details clearly displayed. Emergency drills are also conducted from time to time to make sure that all role-players are familiar with their duties.

It is also important to keep top management abreast of developments with respect to emergency and crisis management. For example, I present a status report to the university management committee as well as to EMT from time to time.

**Hi-Tech Security Solutions**: Looking back, what would be the most important security process/function that you would wish to see implemented or changed before something like this happens again?

**Van der Walt**: In an ideal world, universities should be places that are not sanitised to the extent that universities have seen in the past two years, and where staff and students can express thoughts and ideas freely. Unfortunately, the current situation necessitates security involvement on campus. A solution to the funding crisis to a large extent lies beyond the control of individual universities. That said, on our wish list are bodycams to do live streaming of events to an ops centre (including sound). Time and again we saw that protesters tend to be more violent if they think they are faceless. Once good quality, live streamed video with audio is sent to the ops centre, all indications are that protesters will be more careful and that the level of violence will be less.

The importance of communication to the public on what the government and university management are already doing and will be implementing to meet the needs of students, remains the process/function to counter unacceptable and expensive protest actions.

**Huebsch**: At campuses, more effective access control and prevention of unauthorised access as well as early addressing of potential situations before they get out of hand and become difficult to manage, leading to the need to call in the assistance of the SAPS or other forces. Such early addressing to include the expedition of disciplinary processes, including criminal matters, thus the immediate support and assistance of a dedicated SAPS team becomes an important part of the process.

Also, having government play a more pro-active and tangible approach in assisting institutions of higher learning to overcome the changes that have been brought about to make it possible to better address student concerns in respect of the costs associated with fees.

**Mmapulana**: The police must work with us and guide us during protests. A J.O.G was created in our area during student protests and we worked very well with police, but some of the commanders at campus did not want to listen or work with us. I would like police seniors on campus to have meetings with us and strategise with us.

**Naidu**: You can have a security plan in place, but the issue is that you deal with demonstrators that do not have the same agenda. For example, some want it to be peaceful, others destructive, and others don’t want to conduct activities within the legal limits. What needs to happen is that we only change to a backup plan if it does not work or change certain aspects of the plan to combat certain unforeseen issues.

**Masalesa**: Having a liaison forum established between Protection Services and the Student Affairs Departments. That will ensure that there is constant interaction between the Students Representative Council members and Protection Services. Protection Services will also have the opportunity to demonstrate their value-added services and not to be perceived as the adversaries of the students.

**Hi-Tech Security Solutions** thanks everyone who contributed to answering the questions in this article.
Biometrics makes its mark at universities

By Allyson Koekhoven.

Careful selection and planning leads to benefits beyond security.

In addition to traditional security measures, the adoption of biometric technology in access control systems at tertiary educational facilities is providing knock-on benefits that include examination rolloff procedures and evacuation management and control. Hi-Tech Security Solutions spoke to two industry specialists about current trends in the industry.

Traditionally, within the education sector, the larger tertiary facilities relied on card-based access control systems to provide identification of students and entry into facilities such as campus buildings and student residences. From the late 1990s this was achieved with barcodes and magnetic strips and eventually evolved into RFID. In the past few years there has been a steady and noticeable trend that has seen an increased interest in the deployment of biometric solutions.

According to John Powell, CEO of Powell Tronics, the smaller institutions generally opted for a more basic solution by printing student cards, with a lack of any noticeable access control technology at entrance points. Where these were available, they were usually standalone systems. However, this has changed in recent times with a gearing up to install the latest access control technology to manage their sites.

Powell explains that the main difference between larger and smaller, often privately owned, institutions is that the larger ones are generally situated on one or two large campuses with a number of buildings linked to the system. The smaller institutions are often characterised by a number of smaller sites located throughout the country. Until fairly recently, the connectivity between these sites has been a limiting factor.

Impro's Vikki Vink adds that the use of fingerprint biometrics in particular is fast gaining ground in tertiary educational facilities and is used primarily for perimeter access and thereafter to gain access into internal areas such as libraries, media and IT centres and canteens. This has been identified as a principal drive to ensure the safety and security of students, academic staff and visitors.

The evolution to biometrics on campuses has definitely increased and the added security around biometrics versus card-based access control has been proven on numerous occasions. Since cards can be lost or stolen, there is always a concern regarding the legitimacy of the user. In many instances, buddy clocking has resulted in issues around valid attendance of lectures and examinations.

“One of the benefits of adopting biometric access is that you always have your fingerprint or other biometric ID with you. The obstacle of entry to market for this modality was the high cost but fortunately technology has improved and become more cost effective, allowing educational institutions to see the clear return on investment that it offers,” says Powell.

Best practice in biometrics

One of challenges education institutions face is the high volume of students and access points. Where all departments and buildings are located on one campus, it is easier to secure the perimeter, which in turn allows other areas such as canteens as well as computer labs, with numerous workstations, to be controlled.

Best practice would be to secure these areas by enrolling students on the biometric access control system when they register as a student. This is particularly useful, since one then has the correct information from inception. By integrating the access control data with business systems like SAP or Novell, one creates a single security receptacle for data, resulting in enhanced security.

Although the software is at the heart of the system, and therefore where all the parameters and rules are created, another key consideration must be the type of biometric device used. Increasing demand has resulted in many competitors entering the market, however not all devices are created equal.

Vink cautions that when selecting a biometric device, it is important to take into account the accuracy of the reader, the speed of reading, as well as the average life of the device. Biometrics are a significant investment for any institution, especially compared to traditional RFID units, and therefore the lifecycle costs are imperative. What may seem to be cheaper at the time of tender, can end up being very expensive if one experiences frequent failures, poor reads or even broken devices. Quality is therefore critical in the field of biometrics.

Vink says that in addition to the quality considerations, there is also a need to future-proof the technology as much as possible, especially with regard to the security and integrity of users’ credentials. She cites SEOS mobile credential technology as an ideal solution. The solution delivers secure credentials across a wide range of readers and applications, such as T&A, secure printing and biometric based verification. SEOS protects the storage and use of identities across a broad range of credential platforms and also ensures that no information can be used or read by an unauthorised party.

An added benefit of SEOS, she says, is the ability to choose multiple secure tag choices, such as traditional cards, smart cards, mobile phones, wearables such as Fitbits, along with biometric devices. As the technology expands, so the SEOS-enabled biometric device can offer the institution enhanced functionality into the future.

Powell says that it is wise to select only tried and tested access control solutions which are supported by international accreditation and certification such as that provided by the FBI standard. Choosing a leading brand is always advisable since they are characterised by strong technical support networks. This can be critical when you require onsite assistance.
This should be complemented by an established supply chain to ensure fast turnaround times.

He says that one of the major challenges is to get all the faculties and departments to pull in the same direction. “Once you have consensus on how to move forward, the next challenge is specifying a product that can meet the unique requirements of these large sites, with multiple buildings and thousands of students. Just imagine the logistics around an institution like UNISA, with over 400 000 students and a large staff contingent.

“There are also challenges around the integration of access control software with enterprise resource planning (ERP) software and student software systems. Furthermore, the challenge arising in high-traffic areas where bottlenecks need to be prevented at peak times, has to be addressed. Finally, speed of throughput for functions and examinations is an issue that is also prevalent in universities.”

According to Vink, the biggest consideration is the IT network infrastructure and the associated skills transfer. This is particularly prevalent with many institutions considering IP-at-the-door type installations, where there are increased server demands and strong database and business intelligence requirements.

The bottom line

The route to solving challenges around access control issues at universities is to carefully consider the individual requirements of a particular site and any buildings thereon. The advantages to the institution once any challenges are overcome, are that they can accurately manage attendance and access into specific areas, venues and facilities across any of their campuses.

The ability to derive real-time information in the event of an emergency is a major benefit. “For example by activating threat level, an educational institution can be locked down either automatically or with a few mouse clicks; or all access locations can be opened, depending on the emergency,” says Vink. Critical life-saving features such as this go beyond the traditional security applications.

Vink adds that through the use of handheld biometric units, areas can be limited to a certain number of people or vehicles. An example here is in a parking area, where the system will only allow a predetermined number of vehicles to enter. Such systems can also provide important data that can be analysed to track trends within the facility, in order to assist in future planning.

“The ability to undertake visitor management through the same access control solution is also key, so that there is one single cohesive platform, rather than multiple freestanding systems. The benefit here is that you are able to quickly view the entire site and all people on the site at a glance, rather than having to jump between various monitoring systems,” says Vink.

In addition, as new technologies become available, institutions can quickly adopt these in an integrated system that works off one platform. For example, one can use a mobile phone as an access tag. In individual systems, however, the assimilation of new technology may take longer, due to more bespoke integration being required.

Both Powell and Vink advise consulting with suppliers who have a documented and verifiable customer base in this sector. It is less expensive over the long term to start with high-quality, proven technology that has an established reputation in the market, rather than deploying untested technology.

For more information contact: Powell Tronics, 0861 787 2537, marketing@powelltronics.com, www.p-tron.com.

Impro Technologies, +27 (0)31 717 0700, vikkiv@impro.net, www.impro.net.
Once again, Campprosa delivers

By Andrew Seldon.

Campprosa pulled out all the stops for its 2016 conference in a year when campus security was top of mind for everyone.

The Campus Protection Society of South Africa (Campprosa) held its annual Campprosa International Conference in the second half of 2016 at the Zimbali Hotel, North Coast. This year’s conference was especially pertinent as it dealt with issues campus security professionals were currently facing, such as the outsourcing issue as well as student unrest.

As has become the norm at Campprosa, the conference was well attended with security professionals from across South Africa as well as some African attendees, along with a few international guests. The presentations were targeted right at the heart of what campus security personnel are dealing with and offered insights on a broad range of topics.

One again the event was backed by sponsors who took the opportunity to display their products and services as well as address the audience. The sponsors for this event included Salto, G4S, Thorburn, Sukema, Powell Tronics, Hi-Tech Security Solutions, Altech, Stallion, Axis, FS Systems and AmaziPro.

With two full days of presentations, we can’t cover the event in depth in the pages of Hi-Tech Security Solutions. What follows is a brief description of some of the more notable presentations.

In or out

The first day started with an opening address by the outgoing president of Campprosa, Roland September. During the organisation’s AGM, Derek Huebsch was elected as the new president until 2019.

Following a sponsor’s message, Jenny Reid, director of iFacts, delivered a presentation touching on the contentious issue of insourc ing versus outsourcing. Reid noted that simply switching from outsourcing to insourcing your security staff (or any staff for that matter) was not a simple process and there are risks involved. If universities did not cater for those risks, such as hiring the right people and providing adequate training etc., the organisation could find itself in a tight spot.

Then there is also the question of costs, which might see the number of people employed reduced as the cost benefits of outsourcing are no longer available, meaning the universities would have to make do with less, unless their budgets were increased. There would also be an increase in administration requirements to handle security personnel and their unique compliance requirements.

It goes without saying, but security personnel also add to the administration burden because of the positions they hold. Every security officer needs to undergo a background check to ensure they don’t have a criminal record and to have their qualifications and identities verified. And these are only the first steps in a background check.

PSIRA (Private Security Industry Regulatory Authority) also offered an opinion on the insourcing vs. outsourcing debate. PSIRA’s chair, Prof. Fikile Mazibuko said the authority was not there to prescribe to the institutions present how to run their operations. She said the decision depends on each institution, the costs and their capacity to manage the process of insourcing if that is what they choose. She added that a mixture of insourced and outsourced staff may be the optimal way for universities to start dealing with the issue, again depending on each organisations capacity.

Following Prof. Mazibuko, PSIRA’s CEO, Manabela Chauke followed with insights into the compliance issue. He stressed the need for compliance with the country’s regulations with respect to registering security personnel and said a joint effort was required to ensure the universities were aware of their responsibilities and to assist them in ensuring their staff’s adherence to the regulations.

Chauke also touched on the insourcing debate, again noting that cooperation is required to ensure any outsourcing the institutions require is handled appropriately and within the regulations set by government.

Additionally, Chauke noted that a worrying aspect of the current situation is that of security companies getting involved in public order policing. He stressed that private security operations must restrict their operations in this respect to what the law allows them to do and not allow their employees to go too far in the execution of their duties.

Crime and public violence

Following the AGM and the selection of the new Campprosa executive committee, the last presentation on the first day was from Dr Johan Burger from the Governance, Crime and Justice Division of the Institute of Security Studies. He spoke on what he sees as the two main threats the country faces in terms of security, although he noted there are other issues that must be dealt with if the country is to prosper peacefully.

His presentation included some depressing statistics on the crime situation in the country which showed that in almost all categories of violent crime, the pleasant decrease we saw between 2010 and 2012 (roughly speaking) has reversed and is on the increase again. These increases apply to numerous categories, from house breaking to business robberies and car hijacking, aggravated robbery and the murder rate. And although South Africa is no stranger to public demonstrations, the figures also show that the number of violent incidents in public gatherings is increasing, while the number of peaceful events are declining.

His presentation wasn’t all doom and gloom, however. He noted that the Acting National Police Commissioner (as at September
2016), had started some very constructive initiatives and the outlook from a policing perspective was positive if he was allowed to continue. But that will not be enough. Dr Burger stressed that the country’s economic and political instability must be addressed effectively if the country is to overcome the serious problem of crime and public violence.

Resilience in emergencies
Two international guests delivered a talk and workshop on Emergency Response and Business Continuity on the second day. They were Bernadette Duncan, the COO of AUCSO (Association of University Chief Security Officers), previously with City University in London for 24 years, as well as Peter Brinkley, head of security at the University of Surrey.

Their presentation focused on giving educational institutions the know-how and ability to recover quickly following a disruptive change. They also highlighted various roles and responsibilities in an emergency.

While they had much to say with respect to resilience and the various aspects surrounding the concept, becoming resilient involves preparation (planning), education (train staff and advise students), exercise (rehearse all or parts of the plan), and implementation (using your plans to respond, manage and recover). The workshop on emergency scenarios offered advice to those present that they could take back to their universities and implement in their particular environment.

On the panel
Taking the bull by the horns, Camprosa also offered a panel discussion on the Fees Must Fall issue in which Professor Adam Habib, Professor Francis Petersen and Professor Chris de Beer engaged the audience in a discussion on this touchy subject. The panel members agreed that the discussion between university executives and security operations needs to continue to ensure the safety and security of all on campus.

Some outtakes from the discussion included the understanding that campus

Panel discussion with (left to right) Professor Adam Habib, Professor Francis Petersen and Professor Chris de Beer.

security must become more integrated with the other operational areas of universities. These institutions must also take an holistic approach to their security operations, with proper protocols and processes in place. It is also more important than ever to have proper management information systems in place to assist in the security function.

It’s certain that more demonstrations will take place in future, so it’s important for universities to learn the lessons from 2016 and be ready to deal with these issues. Of course, these issues must be dealt with without hampering the freedoms associated with universities. In short, safety and security must become a strategic imperative for universities going forward.

Randy Burba, chief of public safety at Chapman University (USA) as well as the president of IACLEA (International Association of Campus Law Enforcement Administrators) also attended the event and noted that the Camprosa conference is always a learning experience where security teams can learn and share information. He also said that many problems they face are similar, even if they are situated on separate continents.

The Camprosa International Conference 2017 has already been booked. It will run from 3 – 6 September 2017 at the Kwa Maritane Bush Lodge, Pilanesberg National Park, NW Province. For more information go to www.camprosa.co.za.

Camprosa the ideal platform for Powell Tronics
The Camprosa (Campus Protection Society of Southern Africa) conference has made its mark as the go-to event for campus security. Powell Tronics once again had a strong presence at the conference as both a sponsor of the registration welcoming bags and as an exhibitor. John Powell, managing director of Powell Tronics, says that the company has taken a strategic decision to increase its penetration into the campus security sector and believes that Camprosa is the ideal platform to share knowledge and experience gained in an interactive manner.

John TunSTALL, Camprosa executive secretary says: “Powell Tronics started supporting the Camprosa annual conference in 2010 by sponsoring the Welcome functions. In the past few years Powell Tronics has had specially designed Welcome bags (with both logos) manufactured for all delegates and each containing a bottle of high quality white or red wine and tasty snacks. Their continuous sponsorship has been very valuable and greatly appreciated.”

Powell Tronics’ special projects technical sales manager, Frazer Matchett and Johannesburg sales manager, Alastair McPhail, manned the company’s stand. Matchett says that 79 delegates from universities around the country attended the event. The 2016 conference was characterised not only by a number of trending topics by knowledgeable industry specialists, but furthermore became a catalyst for a group exercise on ‘What to do in an emergency situation’.

During the morning tea and lunch breaks over the three-day period, delegates took the opportunity to view sponsor exhibitions. Matchett says that Powell Tronics’ PT-Rollcall and PT-GUEST proved very popular with visitors to their stand.

Replacing what was traditionally a very manual process, PT-Rollcall, when combined with a biometric fingerprint enrolment on an access control backbone, allows university staff to enrol each student on to the database. This is then used as an attendance register to ensure that the correct student is writing the correct exam in the appropriate venue.
Body-worn cameras on campus

The introduction of body-worn cameras has been a calming and reassuring influence.

The University of Surrey is a public research university located within the county town of Guildford, Surrey, in the south-east of England. The university specialises in science, engineering, medicine and business. The university’s main campus is located on Stag Hill close to the centre of Guildford and adjacent to Guildford Cathedral.

A second campus, at Manor Park, is located a short distance away and has been developed to expand upon existing accommodation, academic buildings and sporting facilities and a world class Veterinary School building which was officially opened by Her Majesty the Queen in 2015. Surrey University currently has 15,500 students, one third resident in campus accommodation and 2000 staff. It is an ambitious and vibrant place with a 24/7 operation.

Security at Surrey University is managed by Peter Brinkley, a former Chief Superintendent with Liverpool Police, who came to Surrey in 2012. He leads a 40-strong in-house security team that carries out foot and mobile patrols across the university estate, and monitors the 200 CCTV cameras. The security team also provides a 24/7 control room and reception where students and staff can report incidents or call for assistance on an emergency number.

Recorded crime is extremely low on campus with less than 100 thefts per year, but all crime is taken seriously and the university has a strong relationship with the local police in Guildford. A great deal of emphasis is placed upon reducing and preventing crime, and working with the police and the Students’ Union to raise awareness on safety and security. Brinkley believes that by reinforcing safety messages, particularly with first-year students away from home for the first time, they have the greatest opportunity to prevent crimes taking place.

**Body-worn cameras effective**

Surrey University is a leading university for technology and has recently opened a 5G technology department. Brinkley and his team recognise the real value of using technology to promote safety and security, and recently introduced body-worn cameras (BWCs) for all of the patrol teams. Many police forces in the UK now use BWCs for patrol, enabling officers to capture best evidence in the investigation of crime.

The introduction of BWCs at the university was initially of concern by some members of staff who feared that the presence of a camera may provoke students. Officers have in fact found the opposite to be the case. Once students become aware of the presence of the BWC, this acts as both a calming and reassuring influence.

Brinkley says, “My staff now wear the cameras every day when on patrol, it is part of their everyday operation. Security staff attending complaints of drunkenness or anti-social behaviour find that as soon as the camera is seen, the situation is often diffused immediately as students do not wish to be seen acting inappropriately on camera.”

In addition to capturing video footage of crime and anti-social behaviour, officers at Surrey University are also able to capture photographs for use as evidence. In cases of criminal damage or road traffic accidents on campus, the footage enables an immediate record to be captured of any evidence. Similarly, health and safety investigations have benefited from the evidence, where staff or visitors report an accident at work; officers capture footage from the scene of the accident, which can then be used to support investigations, for example damage to road surfaces, flooded walkways or poor signage – all of which may be contributory factors in accident investigations.

**Assisting in security cooperation**

The BWCs have enabled the security team to work with the local police in investigating crime and identify offenders who may be trespassing at the university. Brinkley says, “These cameras have made a real difference. Our campus at Surrey University is open to the public and we welcome lots of visitors, but we know that this brings with it a risk of theft. Where we identify unlawful trespassers, we know that they are very uncomfortable being captured on camera so this has a big impact.”

All staff receive training on how to make best use of the cameras, including tactical deployment and communication. When deploying the camera, staff are trained to indicate that the camera is being used and again, this has a real impact on students. A real benefit of this new technology is that it protects both security staff and students, by capturing an accurate picture of incidents as they happen. As such, it is useful to demonstrate to students after the event that their behaviour, language and conduct was inappropriate. This can also be of real value in training new staff and student mentors.

All in all, Surrey University has seen a real, positive difference since the introduction of BWCs. Brinkley said, “I don’t know how we managed without them, they have made a massive difference in terms of improving feelings of safety on campus, and ultimately, improving the student experience.”
Ensuring exam attendance
PT-Rollcall ensures accuracy in examination attendance at educational facilities.

While there are many forms of academic cheating, perhaps one of the most difficult to detect is when a third party sits an examination for a registered student. This is prevalent in large tertiary educational facilities where lecturers do not necessarily know all the students attending their lectures.

Biometrics have been commonly used at primary and secondary school levels in the United States since 1997 and in the United Kingdom and Europe since the start of this century, to provide learners with access to library facilities and canteens, for example. More recently, tertiary educational facilities have adopted biometric verification to ensure that those sitting for examinations are matched with those actually registered for the examination.

According to John Powell, CEO of Powell Tronics, it is important to ensure that any biometric solution deployed to undertake this function is able to communicate with existing educational facility databases. This will obviate the need to cross-reference data manually, not only saving time, but also ensuring high levels of accuracy.

Powell Tronics' PT-Rollcall is designed for use in education facilities and acts as an electronic replacement of manual examination rocall rocall registers. PT-Rollcall, a solution combining biometric fingerprint enrolment on an access control backbone and the education facility's examination system, allows exam invigilators to verify the student's identity using their biometric access information on portable Morpho biometric-enabled devices.

Through PT-Rollcall's integration, prior to each examination starting, the students are required to present their fingerprint in order to check-in at a particular examination venue. On successful identification of the fingerprint template, the student's details, including captured photograph, are displayed on the device for further visual verification by the invigilator. An adaption of the identification process has been included to cater for students with poor quality fingerprints using printed proximity cards with an indication pertaining to the biometric template quality.

PT-Rollcall has been designed in such a manner that it allows for some customisation to best suit the specific educational campus to ensure full compatibility and integration with the university's own student and access management systems. The combined information is uploaded and populated onto mobile biometric devices daily to ensure the most updated data is available at the start of each examination.

A number of South Africa's universities are recognising the benefits of a biometric registration system. Trialled during the mid-year 2015 tests and as a final proof of concept, implemented for the 2015 year-end examinations for a specified group of first year students, PT-Rollcall was used in conjunction with portable biometric terminals. The benefit of using mobile biometric devices are huge, especially in eliminating bottleneck situations for very large venues and giving invigilators, institutions and students the knowledge that all the boxes are ticked.

"As with all technology, the evolution drives the market in seeking the best solution for the job, resulting in ongoing development on the latest available portable/mobile hardware available. As a result we are currently customising the PT-Rollcall software to operate on Android devices that offer aesthetically pleasing usability and user interfaces. Further testing of the enhanced solution commenced at the beginning of November 2016 and the proof of concept will continue into the first quarter of 2017 to accommodate for the exam deferrals due to the recent student unrest," Powell points out.

Depending on which portable device is used, currently the maximum of up to 3000 student templates can be encrypted and stored on each device, providing educational facilities with a quick and reliable way of conducting roll call procedures.

Working in conjunction with the Powell Tronics system management application, Tiberinus, PT-Rollcall allows a seamless link between the access control database and the institution's own student exam database.

PT-Rollcall provides various management reports which will include comparison of the number of students expected to sit for the examination versus the actual number of students present. Other data will include images of the students, the names of invigilators and the venue. Again, customisation is a given and a full audit trail is provided on the software and processes on the mobile device.

"Added value to the obvious benefits of an electronic enrolment process are the elimination of third parties illegally writing examinations for registered students and ensuring that all present, including the invigilator, are indeed in the correct venue at the correct time for the correct examination," Powell concludes.

For more information contact Powell Tronics, +27 (0)861 787 2537, marketing@powelltronics.com, www.p-tron.com
A healthy approach to fire

By Allyson Koekhoven.

Ensuring fire detection and suppression compliance at Discovery Health.

Compliance with occupational health and safety practice is critical to business sustainability. Quite aptly, Discovery Health has taken a strong stand on the deployment of appropriate fire and evacuation safety solutions at its new 120 000 m² head office in Sandton.

Housing 5000 employees from the company’s four buildings currently located in the Sandton CBD, the building will comprise two wings with eight floors of offices plus a ground floor and a feature roof level. It will also offer nine basements with over 5100 parking bays.

Appointed by the main contractors on the project – Tiber WBHO JV – SFP Security & Fire is responsible for the provision of fire detection, voice evacuation, fire telephones and both Argonite and FM200 gaseous fire suppression equipment. Awarded on tender, the company’s appointment as a main service provider was based on a combination of price, product and experience, and called for an EN54 technically compliant system.

According to Dan Lurie, contracts manager at SFP Security & Fire, health and safety considerations are becoming increasingly more stringent on all sites and the sheer size of the Discovery headquarters has resulted in one of the most extensive fire and associated safety technology projects of its kind in southern Africa.

Lurie explains that SFP is networking various fire panels together in one system on the superstructure levels. Essentially, the company is responsible for the fine tuning of the system design (initial design is provided by Trevor Williams Consulting), and technology supply, installation and commissioning on all floors that will be occupied, from the ground floor upwards. The basement levels will be handled by another contractor, using identical technology. This will allow all panels to be incorporated into one network and to be viewed via a single graphical user interface.

Integration is a critical part of the project specification with the voice evacuation system tied into the fire detection system to provide an automatic evacuation system option. Lurie says that given the sheer size of the campus it is important that all of the systems provided contribute to the quickest possible evacuation of the employees.

SFP elected to use Ziton ZP2 addressable fire panels together with ZP7 Series optical and heat detectors for smoke and fire detection with Input / Output addressable devices integrated on the loop to control third-party systems such as the HVAC, start-up and shutdown procedures, and the lifts.

The voice evacuation/PA system is the ATEIS IDAb, with a centralised head end that distributes out to one zone per floor throughout the building. The EN54 certified system offers A/B speaker line wiring for a completely redundant solution. In essence, if there is an open circuit, the speakers are fed in either direction to the break. If a speaker line (A or B) short circuits, it is ignored and does not cause system shutdown as the other loop will still be available on that floor to provide 50% coverage. If an amplifier fails, one amplifier will be available on standby and will automatically kick in and take over the duty of the primary amplifier. The system is fully monitored to ensure continuity of voice addresses.

Lurie says that there will be approximately 2500 detectors, 3500 speakers and 150 interface units deployed, together with 18 distributed and networked fire panels, monitored by a single graphical interface.

Sigtel fire telephones provide an emergency voice communication system in all the fire escape staircases and fire escape lobbies and will result in a coordinated emergency solution operated from a single point. This EN54 compliant system was specified by the project consultants, with 159 outstations offering bi-directional communication.

The client called for fire detection and gas suppressants in the basement data centre. Each of the 10 rooms is protected by clean-agent, high-pressure Argonite. In phase 1 of the project 44 individual FM200 fire suppression systems will be deployed, while a further nine will be deployed in phase 2. FM200, which incorporates an engineered system that uses a fixed nozzle agent distribution network, is a desirable solution for IT rooms since no messy clean up is required if it is activated. It is also non-conductive and non-corrosive and is designed to save personnel levels.

Each of these suppression systems has its own control panel and gas cylinder and is monitored by an addressable panel. In addition, all 10 rooms are also monitored by a VESDA HSSD system to provide early warning.

SFP started work on the project on April 2016 and phases one and two are scheduled for handover in late 2017. SFP is currently busy with the cabling component of the project and will be in full swing with commissioning and testing of the systems in mid-2017.

For more information contact SFP Security & Fire, +27 (0)11 247 7800, dan@sfp.co.za, www.sfp.co.za.
Fire system 2,6 km underground

Moab Khotsong Gold Mine is one of AngloGold Ashanti’s Vaal River operations in South Africa. The mine is located around 180 km south-west of Johannesburg near the towns of Orkney and Klerksdorp. The mine has been in production since 2003 and currently ranks as one of the six deepest mines in the world, with its mining depth ranging between 2,6 km and 3,054 km below surface.

The mine exploits the Vaal Reef (VR) through three mining layers, namely the Top, Middle and Lower Mines. Moab Khotsong employs a scattered mining method with an integrated backfill support system.

Sperosens was recently tasked to design, supply, deliver, install and commission conveyor fire suppression systems at the following high-risk areas at AngloGold Ashanti – Moab Khotsong Mine:

• 102 Level – Overlay and Underlay – Fire Suppression System.

Installation started in September 2016 and will end in March 2017. Once complete, this might well be one of the deepest operational fire detection and suppression systems in the world.

For the application it was proposed that a pre-engineered, standalone suppression system, designed in accordance with NFPA16, be installed at all the high-risk areas. This system is called a Compressed Air Foam System (CAFS) and is designed in accordance with NFPA16: Standard for Foam Spray Fixed Systems for Fire Protection.

The compressed air foam system

The compressed air (nitrogen) foam system is a fixed automatic fire prevention, detection and suppression system, consisting of a control unit, fire and heat detectors, a set of discharge spray nozzles, a pressurised water/suppression agent tank, a high-pressure nitrogen cylinder, a number of solenoid valves, and pressure and level switches. The unit can also be interfaced and displayed onto the SL2010 fire detection telemetry system or scada system.

The foam spray fire suppression system is a stand-alone, pre-engineered, modular fire suppression system that can be configured to supply various quantities of nozzles, from a minimum of two nozzles, up to a maximum of twenty-one nozzles per single cylinder system. The normal operating pressure of the conveyor belt tank is designed such that the discharge nozzles should operate at a constant adjustable discharge pressure of between 3 and 10 bar, thus allowing for a balanced and equal discharge from all the nozzles, depending on the specific design application and duration discharge required.

Principle of operation

A vessel is filled with a mixture of water and a foaming agent and is pressurised using a standard nitrogen cylinder. Two sensors are used to detect overheating:

• Plumber block temperature sensor – to detect the overheating of bearings.
• Infrared temperature sensor – to detect overheating of pulleys.

In addition, a Triple Spectrum (IR) Infrared Flame Detector is used to detect flames. The system will automatically discharge the vessel contents through a solenoid valve, piping system and correctly placed nozzles when a fire alarm is generated.

Installations of CAF solutions have been successfully implemented on surface conveyor belts since 2012.

For more information contact Marihette Hattingh, Sperosens, 086 177 3767, marihette.hattingh@spero.co.za, www.spero.co.za
The toughest fire challenges?

By Phil Barton, UTC.

Techniques and solutions for difficult or complex environments.

While today’s range of smoke and heat point detectors and fire alarm control panels provide excellent fire detection for most buildings, some sites demand more specialised solutions. Such sites, including industrial settings, complex corporate buildings, major infrastructures and areas where harsh environmental conditions prevail, may require the deployment of a much wider range of detection technologies and techniques.

There is a wide range of tried-and-tested detection solutions available and a combination of detection techniques can often yield the best results. Different types of detectors, working on different principles and with particular advantages, can be interfaced to develop a unique solution. For example, some environments encompass a wide range of temperatures and atmospheric conditions as well as conditions that change rapidly.

Facilities such as manufacturing sites, power plants, and data centres may also include risk profiles that require rapid detection of incipient fires or minimisation of false alarms. In these locations, device performance may be the most important factor in the choice of detection technique. Degradation of detection devices can be resolved by using ruggedised sensors or by removing the detector from direct contact with the harsh environment.

Simple but effective

Point detectors are often the preferred choice for general office and residential spaces, providing an adequate balance between detection performance, cost and false alarm resistance. But they should not be overlooked when it comes to more difficult sites. Typically, these detectors use electronic thermistors to sense heat and light beams to detect smoke particles.

For more demanding environments, false alarm immunity can be achieved by using a combination of multiple devices that offer smoke and heat-sensing capabilities. Sensor information, absolute readings and rates of change are then assessed by selected algorithms to either speed up detection response or provide more reliable alarms.

By their nature, point smoke sensors are vulnerable to contaminants in their vicinity and may require enhanced maintenance and replacement regimes. System designers should also be aware of the full range of specialised sensors. For example, ruggedised heat probes can be located in places such as cooker hoods that would not be suitable for traditional point detectors.

No wiring?

In many applications, the challenge comes not from the environment, but from the limitations placed on the installation. A point-type detection system requires cabling through a risk area to link all of the detection devices to the fire alarm control panel. This can be a challenge in sites where the fabric of the building does not lend itself to the routing of cables or drilling of walls.

Wireless detection technologies have become more robust and reliable. They provide point-type detection and the interfacing of other detection devices without the need for cabling. Many systems offer a simple loop interface module that can expand an existing wired loop by adding wireless devices. Other systems provide a hub and cluster solution which can create a completely wireless detection system comprising multiple loops.

Robust, effective sensor cable solutions

Linear heat detection is a simple, dependable technology, which is ideal for applications such as floating roof fuel storage tanks, conveyor belts, cold stores, tunnels and rolling stock. Its robustness makes this technology a cost-effective solution for many applications.

The range of linear heat detection technologies has grown over the years from the simple digital technologies using two core cables, which short circuit at their alarm temperature, to analogue systems that provide variable alarm temperatures, pre-alarm and alarm thresholds. Fibre optic systems can provide absolute temperature monitoring.

Many of these systems incorporate control units, which identify the location of an alarm event along the length of the sensor cable allowing a rapid emergency response to an incident.

With a wide range of protective outer sheaths providing environmental, chemical and mechanical protection, there is a linear heat detection solution for most environments, even the harshest. Linear heat detection sensor cables, unlike many other forms of detection, can be installed within hazardous areas while the control units are located in a safe area.

Aspirating smoke detection (ASD)

Aspirating smoke detection systems have increasingly become the system of choice in applications where point detection systems cannot cope with the environmental conditions. Problems such as high airflow in forced air environments, stratification in high-ceilinged areas as well as high and low temperatures can be overcome using ASD.
ASD systems use a distributed pipe network containing sampling holes connected to a detection unit that contains a fan and high-sensitivity detection chamber. Air is drawn from the protected area along the pipework by the fan to the detection unit. Flexibility in the design of the aspirating pipework ensures an early detection of smoke by placing the sampling points in the best locations.

The detection unit can be located outside the risk area where it will not be affected by adverse environmental conditions. The air can then be treated before it enters the detectors by inserting filters. These can mitigate the problems caused by extremely dusty environments, for example. Similarly, heater boxes can offset the effects of extremely cold environments.

One of the main advantages of ASD systems is the cost of ownership. Maintenance, repairs and testing are often quicker and easier than with other systems as the detection unit is mounted at low level. This removes the need for working at height and the additional equipment and procedures this would require. For restricted access areas, the detection unit can be mounted externally thus maintaining the security of the risk area.

Using ASD can have advantages for many different applications. At critical sites such as data centres, the ability to provide an early indication of smoke is essential for protecting high-value equipment and reducing the potential cost of business downtime. In other situations, extra time may be needed to enable controlled evacuations. This would be particularly important in public buildings where large numbers of people may be present. And where access for maintenance is an issue, ASD can prove especially useful.

Rapid detection of visible flame
Smoke detectors can be very effective in areas where smoke is generated, but are not as effective where clean-burning fires are a possibility. Liquid fuel fires generate a flame but not necessarily smoke until other forms of solid fuel are involved. Line of sight flame detectors provide a quick alarm response to the presence of a flame by detecting either the ultraviolet (UV) or infrared (IR) radiation. It’s important to note that UV and IR radiation can be generated by many sources so it is essential that the risk of false alarms be mitigated. The combination of multiple sensors, such as UV/IR, dual IR, and triple IR, can improve performance while reducing the false alarm risk.

Flame detectors are generally installed in extremely hazardous areas where the main risk is a liquid chemical or fuel fire, such as in fuel storage depots or aircraft hangars. These are areas where the presence of any flame, no matter how small, can be catastrophic. For this reason many flame detectors are available in Ex certified enclosures which, unlike many other forms of detection, allows them to be installed in potentially explosive atmospheres. Unlike many other forms of detection, these can be installed within the hazardous environment. Flame detectors are suitable for open areas, either indoors or outdoors.

Linear beam as an alternative to point detectors
One of the restrictions of point type detectors is that the height of installation can affect performance. In buildings with large open areas, such as factories and warehouses, linear beam smoke detectors are a good solution.

Consisting of a transmitter and a receiver, beam detectors work through light obscuration. The transmitter sends out a beam of infrared light which is detected by the receiver. The generation of smoke within the risk area will begin to obscure the infrared light beam. When the level of smoke reaches the point that the receiver can no longer detect enough infrared light, an alarm is activated.

Beam detectors can effectively cover distances of up to 100 metres. Previous installation issues with the alignment of the transmitter and receivers, and misalignment due to flexing of the building structure, have been corrected by auto-aligning the beam detectors.

Good old sprinkler bulbs
Let’s not forget that sprinkler bulbs that initiate sprinkler valves are a robust and effective technology for industrial environments. Sprinkler systems can be expensive but offer detection of a fire as well as fire fighting media to suppress or control the spread of fire.

Hazardous environment solutions
Where there is a risk of explosions (including all areas defined as hazardous by BS EN 60079 and its sub-parts), it is essential to use equipment designed and approved for such areas. There are three main types of equipment categories for hazardous areas:

1.) Intrinsically safe: Electrical equipment that has been designed to limit the electrical and thermal energy it generates, preventing it from causing ignition of a flammable or combustible atmospheric mixture.

2.) Increased safety: Equipment that is designed to eliminate the possibility of sparks and hot surfaces which would be capable of igniting a flammable atmosphere.

3.) Flameproof: Electrical equipment housed in an enclosure that will contain an internal explosion preventing the ignition of a surrounding explosive atmosphere.

Many other categories for hazardous area exist such as purged and pressurised, encapsulation and oil immersion. It is the responsibility of the facility owners to classify areas where potentially explosive atmospheres may occur, defining them as either zone 0, highest risk category, or zone 1 or 2, which are lower risk categories. Due to the risk associated with hazardous areas, it is important that installers and designers be experienced in this type of application and work closely with the facility owners to ensure safe practices are followed.

System integration
The emergency procedures that are implemented when an alarm is activated by one of the many detection systems mentioned above are also critical. The effectiveness of this implementation can be enhanced by interfacing the site’s fire and security systems into a seamlessly managed single solution.

Many advantages can be gained from interfacing fire and security solutions with a central control and monitoring user interface such as the UTC Fire & Security ATS8600 Advisor Management Software. ATS8600 brings together video, intruision, access control and fire systems through a graphical user interface. In the event of fire alarm activation, a remote view of the area where the alarm has been triggered can prove invaluable.

There are many other benefits to the software. For example, ATS8600 can provide connectivity between the detection zone in alarm and any security cameras located in the area so that a remote view is obtained. This can give valuable information for the emergency services including confirmation of a fire and the approximate size of the fire, without putting any members of staff at further risk.

The ability to visualise and manage both the fire and security systems on a site can significantly enhance the effectiveness and safety of a response during an emergency situation.

Conclusion
It is important to note that there can never be a ‘one size fits all’ fire detection solution as buildings and the activities carried out within them all vary. Therefore, it is essential for system designers to be aware of the wide choice of technology, products and solutions to provide the best level of performance for any situation.

All sites must have a risk assessment done to highlight areas requiring special consideration. And, of course, to ensure the suitability of a particular detection type for an application it is also advised that a site survey be undertaken prior to any designs being completed.

For more information contact UTC Fire & Security, +27 (0) 11 579 7300, utcfs.ssa@fs.utc.com, www.utcsecurityproducts.eu.
Improved life safety awareness

New research from Hochiki Europe shows improvements in building owners and managers’ knowledge of maintenance requirements for life safety systems.

A 2016 study of European Installers found that the number of building owners and managers unaware of the legal requirements surrounding life safety system maintenance has halved. The company’s 2015 research found two in five, or 46%, had no awareness, however that figure has dropped to one in five, or 22%, in the past 12 months.

The study also showed an increase in the number of customers’ installers visited with up-to-date fire detection and emergency lighting logbooks. In 2015, two fifths of customers (40%) failed to have an up-to-date fire detection logbook. This figure now stands at less than a third (30%). The number failing to have an up-to-date emergency lighting logbook has dropped even further, falling from over two thirds (67%) in 2015 to under half (48%) in 2016.

Despite the improvements in these key areas of maintenance, the number of building owners and managers experiencing false alarms showed little change, dropping just 1%, from 29% in 2015 to 28% in 2016.

Equally, the number of installers encountering buildings where customers had changed the use of their spaces, but failed to adjust their life safety systems accordingly dropped only slightly, reducing from just over half (55%) to exactly half (50%). More worryingly, this year failing to update the system correctly was the most common issue installers found when visiting a customer site.

The top five fire maintenance issues encountered by installers in 2016 were:
1. Change of building/room use without correctly altering the fire system (50%).
2. Inadequate logbook records (44%).
3. The original installer didn’t install the best system for the environment (40%).
4. Detectors need cleaning (33%).
5. Detectors need replacing (27%).

The top five emergency lighting maintenance issues encountered by installers in 2016 were:
1. Broken/faulty lamps (44%).
2. Inadequate logbook records (42%).
3. Inadequate emergency lighting signage (39%).
4. Batteries not charged in emergency lighting units (35%).
5. Inadequate lux levels (25%).

Tracy Kirk, GM of sales and marketing for Hochiki Europe, commented: “Our annual study shows a marked improvement in both understanding and meeting maintenance requirements among building owners and managers. This suggests that, as an industry, our efforts to educate and train those responsible for maintaining life safety systems is proving successful.

That said, we acknowledge there are still some serious gaps to continue addressing, and while these are encouraging results we cannot be complacent. Ensuring the legal requirement for keeping up to date logbooks is met, the correct system is in place and reducing false alarms, are all vital to keep people safe. We will continue to provide training and information that can help our installers educate even more building managers and owners on the importance of life safety maintenance and the correct ways to carry this out.”

For more information contact Paul Adams, Hochiki Europe (UK), +44 1634 266 568, padams@hochikieurope.com, www.hochikieurope.com.

SecuriFire fire detection system

The SecuriFire fire detection system is setting new standards in fire prevention.

What does a small research laboratory have in common with an industrial company? Well, both would be severely affected if a fire broke out. And for both, the safety of staff and customers as well as their assets is paramount.

The pace of developments in security technology is soaring, and that is true also of fire detection technology. Securiton is a pioneer when it comes to fire prevention through even swifter responses and greater system availability. Its latest achievement – the SecuriFire fire detection system – is setting new standards in fire prevention.

The standalone version SecuriFire 1000 is ideally suited for small and medium-sized businesses of all kinds. The network-compatible small-scale control unit SecuriFire 2000 eliminates the sort of unsettling risks that larger companies might otherwise have to face. Large companies rely on the protection provided by the fully redundant SecuriFire 3000 system. Not only is it possible to connect up to 14 addressable loops per control unit, up to 16 control units can be networked into a homogeneous overall system.

Uniquely positioned to offer optimal FIRE DETECTION solutions for all industries across Sub-Saharan Africa

PRODUCT RANGE

- Aspirating Smoke Detection
- Conveyor Belt Detection
- Emergency / Evacuation
- Extinguishing Panels
- Fire Cable & Clips
- Fire Control Panels

BlazeCut Automatic Fire Suppression Units operate fully independent, are easy to install, maintenance-free and ideal for:

- Engine compartments of:
  - vehicles,
  - machines,
  - pleasure boats
- Electrical, server, and battery cabinets
- Vending machines, POS machines, ATMs
- Small generators

SERVICES OFFERED

- Outstanding Customer Service
- Repairs & Technical Support
- Full Training on Fire Detection Systems, including SAQCC Certified Training
- Locally Designed and Manufactured, as well as World-Class Imported Fire Detection Equipment
- Assistance with System Design and Budgetary Costing

HEAD OFFICE - JOHANNESBURG
T +27 (0)11 794 0144  E info@technoswitch.co.za
Cusonia Park, Ridge Road, Laser Park, Johannesburg

CAPE TOWN
T +27 (0)21 948 4575  E infocpt@technoswitch.co.za

DURBAN
T +27 (0)31 268 8843  E info.cn@technoswitch.co.za

ISO 9001:2015 Certified
BlazeCut automatic fire suppression

The BlazeCut system is designed to protect small enclosures susceptible to greater risk of fire. It operates automatically, without a power supply, through detection of high temperatures. When the temperature in the protected enclosure rises to a critical threshold, the heat sensitive BlazeCut tube melts down at the point where the affecting temperature is the highest. Melting of the BlazeCut tube creates a hole, thereby releasing the extinguishing agent in the tube directly onto the source of the fire.

BlazeCut uses two different extinguishing agents: for vehicle application an HFC236A agent is used, and an HFC227 agent for non-vehicle applications. The main benefits of BlazeCut include a long shelf-life and no maintenance. It is perfect for non-occupied spaces and no training is required for the simple installation. BlazeCut can operate in temperatures of -40°C and the activation temperature is around 120°C.

BlazeCut is suitable for a variety of applications and can be used in Class A, B and C, as well as electrical fires. Additional components are available for monitoring purposes. These include a pressure switch that sends a signal when the pressure in the tube drops, and can be linked to a fire panel or directly to a PLC.

Typical applications include:
- Engine compartments of vehicles, machines, pleasure boats.
- Electrical, server, and battery cabinets.
- Vending machines, POS machines, ATMs.
- Electrical charging stations.
- Enclosures with audio-video devices.
- Small generators.

For more information contact Technoswitch, +27 (0)11 794 9144, info@technoswitch.co.za, www.technoswitch.co.za.

Advisor Management Software

Security and facility management has evolved into a complex set of business functions, which all need to be managed, taking safety and security of the staff, visitors and physical assets as a priority. There are numerous factors driving complexity: multiple sites, remote locations, flexible working hours, number of employees and visitors, as well as evolving needs.

Only an integrated management solution is able to cope with this evolution, providing facility and security managers with a clear view and control over these different functions. Imagine one interface to manage and control all of your security needs on-site or remotely, on various premises, ranging from intrusion and fire detection to access control and video surveillance.

The Advisor Management System supports full integration of the FP1200/FP2000, 2X, ZP2 and iFP fire alarm panels for event monitoring as well as control over the fire alarm system installation. It provides the operator with an intuitive graphical user interface, featuring graphical plans with events dynamically displayed on screen to assist in the rapid location of a fire. This allows for improved response time to fire events and other hazards, thus reducing risks to life, property or the environment.

In case of a fire alarm, the location of the alarm will instantly appear on the screen. Activation of a live video stream allows verification of the presence of a fire and if needed, other video streams can be selected directly from the floor plan. When a raging fire has been confirmed, doors can be unlocked, sounders can be activated, elevators can be brought to the ground level, all while verifying the chain of events with the video system connected.

One database for all functions linked to events and where access rights can be altered, eliminates chances for error. Advisor Management Software also supports:
- Digital video surveillance.
- Intrusion detection.
- Access control supporting multiple sites.
- Vending machines, POS machines, ATMs.
- Electrical charging stations.
- Enclosures with audio-video devices.
- Small generators.

There is also a mobile application for iOS, Android and Windows. Features include:
- View the fire network status
- Reset a fire network or a control panel
- Sound or silence sounders
- Enable or disable features or devices
- Perform a one-man walk test
- View system events

For more information contact Security & Communication Warehouse, +27 (0)12 653 1005, marketing@securitywarehouse.co.za, www.securitywarehouse.co.za.
Safe, Cost-effective, Environmentally Friendly Fire Solutions for your Peace of Mind

SPERO SOLUTIONS:

- Fire Detection Solutions
- Fire Suppression Solutions
- Fire Extinguishing Products
- Fire Equipment Monitoring
- Temperature Measuring
- Environmental Monitoring
- Fire Safe Design

Product Innovation & Service Excellence with each Fire Prevention Solution Supplied
www.spero.co.za • info@spero.co.za • +27 12 665 0317
**Waterproof fire detectors**

Heat detectors are normally used in rooms where the temperature can be expected to rise rapidly in case of a fire, or in places where smoke detectors cannot be used. The 6000 series heat detectors are intended for outdoor or indoor use in high humidity areas.

The 6000 series detectors are conventional fixed temperature heat detectors, i.e. they will give an alarm within a response temperature range in accordance with EN54-5:2000. The sensing element is a heat pick-up shield and a bimetal switch. An LED on the detector will light up when the detector activates. All detectors support an output for a remote indicator.

All detectors are latching, i.e. they will not be automatically reset if the temperature, after the alarm, falls below the detector’s static response temperature. The detector’s LED and a connected remote LED will be lit until the detector is reset via the C.I.E.

All electronic components are mounted in a grey waterproof detector housing and fitted to the supplied connection box. The connection box has three cable inlets. Three compression glands and a silicon gasket for IP67 protection are supplied with the product.

**Standard Features**
- Fixed temperature alarm level.
- ATEX compliance (6295 and 6296).
- Waterproof (IP67).

For more information contact UTC Fire & Security, +27 (0) 11 579 7300, utcfs.ssa@fs.utc.com, www.utcfssecurityproducts.eu.

---

**Fire panels from Security Warehouse**

Aritec fire panels are supplied in local language with user interface, with fire routing controls and two loops that support up to 256 devices in 128 zones. They have standard four supervised sounder/firerouting outputs, which can be used as freely programmable outputs. In addition, two conventional relay outputs and two supervised outputs work in pairs and are dedicated to common fire and fault conditions. Two user-configurable inputs for monitoring and control are also available.

The panel supports an extra two loop boards that brings the panel to up to 256 zones with four additional programmable outputs. Add a network board to create a maximum of 32 nodes/32 loops network of fire panels and fire panel repeaters (including conventional fire panels and fire panel repeaters up to a maximum of 64 conventional zones). Last but not least, in case separate zone indications are required, a 20 or a 40 zone fire/fault LED indicator board can be mounted in the panel or repeater with ample space for custom text.

The Ziton and Aritec Panel series life safety control systems are bringing the speed and functionality of high-end intelligent processing to small- to mid-sized addressable applications. They feature a contemporary design that fits with any décor. With the addressable detection and a full line of easily configured option cards and modules, USB and Ethernet connectivity, these quick-to-configure systems offer versatility that benefits building owners and life safety system installers alike.

For more information contact Security & Communication Warehouse, +27 (0)12 653 1005, marketing@securitywarehouse.co.za, www.securitywarehouse.co.za.
Taking aim at number plate recognition

By Andrew Seldon.

Locally developed number plate recognition solution without the hardware hassle.

Hi-Tech Security Solutions’ readers were introduced to GateBook, a locally developed visitor management system last year in the Residential Estate Security Handbook. In the original article we noted that one of the GateBook modules is automated number plate recognition (ANPR), which residential or business estates can use to compare cars requesting entry with a hotlist of undesirables which should be denied access to the estate. Alternatively it can be used to simply keep a record of what vehicles entered and exited the estate and the associated driver’s licences that were scanned.

This is useful, but a limited use of ANPR and Grant Hancock, MD of GateBook, believes the process could be expanded to increase security levels on a far wider scale than an estate. He says traditional ANPR is reactionary and allows you to react after the event, not immediately. SNIPR is different.

GateBook’s ANPR system, SNIPR, is connected to the SAPS database of suspicious vehicles as well as many other sources. These sources can be existing databases of vehicles, live camera feeds, handheld devices and so forth. The system is already integrated into Hikvision LPR cameras.

Once a number plate is received by the SNIPR server, it is compared to the plates on file and on the SAPS database. If it turns out to be a suspicious vehicle, the security teams at estates (or shopping malls, business campuses or anywhere there is a constant flow of vehicles), can be prompted to take the relevant action.

The action in this instance is immediate. A vehicle with a number plate that raises an alarm can be prevented from entering an estate or business premises or, to avoid endangering innocent people, it can be allowed to enter until it is confronted by the police or a security team.

SNIPR can be used with different cameras and surveillance systems, it does not require users to buy special equipment. It can also be used with a management system (like GateBook) that provides step-by-step instructions on what process must be followed when a suspicious number plate is recognised.

Hancock explains that SNIPR is not competing with current ANPR systems as it does not read number plates, but the company has written an API that can interpret number plate information from third-party systems. Hancock says GateBook will write integrations to connect to any third-party systems willing to provide number plates to SNIPR.

The system does not record video footage either, only those images associated with the ANPR recognition, and these images are only stored for a short time.

SNIPR has been put through its paces in a number of pilot environments and is being rolled out to a growing number of organisations.

For more information contact GateBook, info@gatebook.co.za, www.gatebook.co.za.
ANPR’s local potential

ANPR offers both public and private organisations numerous benefits for efficiency and security.

While Automatic Number Plate Recognition (ANPR) has been around for decades, the technology has grown in leaps and bounds in recent years with increasingly more integrated solutions providing an enormous benefit to law enforcement agencies and security services providers around the world.

ANPR works by reading vehicle registration information in real-time as vehicles pass by the camera. The impressive developments in IP camera technology over recent years mean that these cameras can capture high-definition images regardless of vehicle speed or quality of light.

ANPR software can be used to cross-reference license plates against law enforcement databases to identify stolen or unroadworthy vehicles, as well as criminals that have had their vehicles flagged in the system.

According to Gus Brecher, managing director of Cathexis Africa and business development director of Cathexis Technologies, ANPR offers a significant potential for private and public applications, and when integrated with other security solutions, it is potentially an extremely powerful law enforcement tool.

CathexisVision provides an ANPR solution for both low and high-speed applications. The ANPR software allows for the identification and capturing of number plate information via cameras and databases.

“This provides 24/7 access to users who can compare images captured to blacklists or whitelists and take immediate appropriate action against these comparisons,” says Brecher.

“The ANPR feature is well-suited to any parking/access control application as well as any high-speed freeway detection requirements. The CathexisVision ANPR feature can be used in over 200 countries worldwide.”

For a simplified user experience, the ANPR feature allows for the simple setup of cameras at any height or angle, which will not interfere with accurate identification capability.

Licence in the cloud

Visec announces embedded licence plate recognition using Hikvision cameras, eliminating traditional hardware.

Visec, creator of the Viscend surveillance software suite and the licence plate recognition cloud network in South Africa (LPR CLOUD SA) announced it has released software technology making license plate recognition to the cloud more affordable. The Visec solution eliminates costly computer hardware associated with implementing license plate recognition systems.

The result will provide a standalone alone licence plate recognition solution engineered for easy capturing, analysis and recording of licence plates all built into the camera and automatically sent to the LPR CLOUD SA. No PC or server is required, just a regular Internet connection.

Visec has collaborated with Hikvision, which engineered the camera that will be powered by Visec’s LPR CLOUD SA technology.

“This lower cost architecture offers the potential to significantly extend coverage of the LPR CLOUD SA to reach an even wider geographic location. Such a significant cost savings will also enable a rapid global market expansion of the Viscend Cloud LPR that was not possible before,” says Gary Scagell, CEO of Visec.

The Visec standalone LPR camera is powered using edge technology which allows software developers to write camera apps, in a similar fashion to a cellphone running an app. The Visec licence plate recognition app will run standalone using the Hikvision camera’s processor and memory.

“We have the ability to identify specific areas of growth in viable niche markets while ensuring our clients have the most advanced solutions,” says Jason K. Bordbar, senior VP of sales and marketing, Visec USA. “Now we are able to offer a total cost of ownership for the Viscend Cloud LPR at a 75% price reduction for typical deployments, thanks to this new camera technology. Such a drop in price point will enable Visec to implement cloud-based LPR solutions more effectively across emerging markets.”

For more information contact Cathexis Africa, +27(0)31 240 0800, sales@cathexisafrica.co.za, www.cathexisvideo.com.
Parking with Panomera

Parking at the airport is safe when the lot is covered by effective surveillance technology.

There are many reasons for travelling and just as many things to worry about ahead of departure. While some issues, such as bad weather or technical failures are beyond personal control, other concerns can be remedied. Since 1995, Italian airline passengers who favour driving their own vehicles over using public transportation in order to get to the airport have been entrusting their vehicles to ParkinGO for the duration of their trips. At more than 20 locations across Italy – including seaports – the company is providing guarded parking spaces and shuttle services, making sure that passengers don’t have to worry about parking anymore.

The responsible project managers at ParkinGO knew exactly what they wanted from the new video system. Obviously, the entire office and parking area would have to be covered to ensure the safety of all vehicles, but the system would also have to facilitate access control as well as help monitor adherence to traffic rules. All-in-all, the following specifications were made: comprehensive observation of all covered and uncovered parking spaces, camera coverage of entries and exits allowing for a 360-degree view of passing cars, and number plate recognition at the driveways with database storage of the registration data. The latter was particularly important to ParkinGO from an insurance-legal perspective as it would allow them to prove that a specific vehicle was returned to its owner in the exact same state as when it was originally parked.

For securing the outdoor areas of the car park, the project team chose to employ the multifocal sensor system Panomera, a camera technology which was specifically developed for the all-encompassing surveillance of expansive areas. The ParkinGO management was given a preliminary on-site demonstration of the innovative system's quality and capabilities, which confirmed the initial choice.

In order to capture all vehicles entering or exiting the premises from every angle, both driveways are each equipped with five high-definition dome cameras featuring automatic day/night operation. They provide detailed images in full HD quality. The video system is recorded on two dedicated high performance server appliances.

In addition to handling Dallmeier devices, one of the servers was configured to also record third-party cameras which were installed in selected areas across the site. Using specially developed VideoIP client software, the recordings can be evaluated quickly and easily.

Investing in a video security system requires thorough considerations and careful financial planning. ParkinGO eventually concluded that there were a number of convincing reasons to choose a Dallmeier solution. Three reasons were particularly decisive, namely, the user-friendliness of the systems, the high savings potential of the Panomera with regard to the costs of the technical infrastructure required for security systems as well as the possibility to remotely operate all functions of the system. The remote operation is even possible with only limited bandwidth available. In that case Dallmeier’s proprietary transfer method PRemote-HD is used to transmit video data.

For more information contact Dallmeier Southern Africa Office, +27 (0)11 510 0505, dallmeiersa@dallmeier.com, www.dallmeier.com.
2017 security outlook

By Andrew Seldon.

What’s in store for 2017 for the physical security industry?

2017 is off to an interesting start, both in South Africa and internationally, but what does the year hold for the security industry? Hi-Tech Security Solutions asked two industry players for their opinions on the coming year and what they were expecting.

When it comes to what technology we should keep an eye on, Rob Anderson, MD at Rob Anderson & Associates, says there are three areas to consider. He says there seems to be significant movement in the VMS (video management systems) world as these applications continue to grow and cover more ground in terms of what they can manage and the functionality they offer.

Moreover, biometrics is also important and Anderson says the promise of improved face recognition and voice activated access control should produce some interesting news in the coming year. Finally, the Internet of Things (IoT) ‘seems to be starting to show its face’, which will have a significant impact on the security and other markets.

Brent Cary, regional sales manager for Genetec, expects 2017 to see a continued rise in the importance of subscription and managed services, with end users in security placing emphasis on outcome-based ownership versus perpetual licences. “In addition to the significant cost savings and flexibility associated with this type of ownership, moving more data and computing to the cloud will allow organisations to transfer a big piece of their cyber security risk to companies who have global teams dedicated to maintaining data security.

“Also, with the rise of cyber security risks affecting the physical security market, organisations will put more focus on establishing rigorous risk assessment and product lifecycle programmes in order to benefit from the latest technology available to counter those risks. They will be much more demanding on manufacturers and system integrators regarding the solutions they are installing on their network.”

The cyber question

The cyber security question is naturally one that will require much more attention in the physical security market this year. Unfortunately, Anderson says, “there is generally a total lack of understanding in this sector. When your cellphone is stolen, you get emotional. When your data is stolen you don’t even realise it has happened. If you get a virus on your system then you get upset and rebuild the system. It would seem that there is no urgency to address this problem.”

“The fact is that we have more IP devices and systems that are improperly secured. The responsibility for cyber security doesn’t fall only on IT departments, every player in the physical security market, from manufacturers, to consultants, integrators and end-users will have a part to play,” adds Cary.

The challenge, therefore, is going to be one of education. The industry needs to inform customers on what is insecure, teach them how to avoid pitfalls and how to protect themselves.

“2017 will also be a year of awareness about cyber accountability,” notes Cary. “The burden of responsibility needs to rest with the people who make us think we are secure when in fact we are not. Rising cyber crime and its increasing threat to businesses has organisations taking direct action to mitigate their risk.”

So where’s the pot of gold?

The common view of the security industry is that it is a great industry to be in because of the uncontrolled crime levels in South Africa. For those in the industry, however, while there is business to be found, it is also a tough industry with price all too often being the deciding factor in buying decisions, often to the detriment of quality and performance.

When looking at which sectors or industries will be the most active when it comes to physical security, Anderson expects to see the private sector leading the way due to the reducing support from SAPS. Within the private sector, Anderson believes the biggest growth areas will be the residential and retail sectors.

However, he says the market is now calling for end-to-end solutions that include technology, response and investigation services. “The response component even includes medical response. There is also a call for specialist, trained personnel to react to big security incidents. This integrated security solution will be everything except the gaol and the courtroom.

Cary sees organisations looking for more return on their video surveillance investments by collecting analytics and customer intelligence gathered by their security systems. Genetec, for example, will introduce a retail business intelligence system in 2017 that will offer people counting, flow management and customer retention data. Significantly, the system will include analysis features that provide end-users with easy-to-read reports on their business. In general, he says the conversion of security data into intelligence will become more important going forward.

What are your expectations for the security industry in 2017? Join the ranks of Nostradamus and let us know what you think will be the main trends in the coming year by sending an e-mail to trends@technews.co.za
Systems become platforms, deliver more value

By Neil Cameron, Johnson Controls area general manager, Building Efficiency – Africa.

Security systems are creating value for the organisation that goes beyond safety and securing assets.

Security will remain a priority for companies throughout 2017 and beyond. The good news is that security systems and platforms are becoming smarter, allowing organisations to do more, creating value for the organisation that goes beyond just ensuring safety and securing assets.

Key security trends for 2017 will include the following:

- Systems continue to move into the realm of open security platforms that allow integration of multiple solutions, such as access control and CCTV, and away from stand-alone or proprietary security solutions. The drivers for adoption of open platforms are greater control, cost efficiencies and greater integrated functionality. For example, being able to cut energy consumption by having a system in place that understands when parts of the facility have zero occupancy and the lights and air conditioning can be switched off. Companies with dedicated systems – eg, an access control system that only opens and closes doors – need to look at the possibilities of integrating these solutions to a platform.

- Rules-based systems are emerging that add significant value. Security solutions, such as access control, can now integrate into and help update and drive enterprise systems, such as workforce and staff management systems. For instance, a rules-based access control system that draws on enterprise information can define where an individual can go and what they can do based on rights assigned in an HR system. It can also auto-update rights as they change.

- Smart analytics and machine learning will become more prevalent. With more data available, there is greater opportunity to begin mining it and making sense of it. Video analytics, for example, is becoming quite advanced. CCTV and video management systems now include motion detection, camera signal loss detection, camera obstruction detection, alerting when there is activity in designated restricted zones, automatic licence plate recognition, dwell time and loitering alerts, and people and vehicle counting.

- Security platforms will start giving value back. It has become faster, easier and cheaper than ever before to interface into platforms and systems that are already deployed. The ability of systems to connect to multiple sensors and readers is now also given. As systems become more intelligent, basic functionality, such as passive surveillance in a retail environment, will be exploited to enhance operations, security and other business-related functions. For example, the surveillance capability won’t only protect assets, it can be used to identify where people spend time in a store and if the correct merchandise is available on particular shelves, or if lines at tills are getting too long and more cashiers need to be deployed.

For more information contact Johnson Controls, +27 (0)11 921 7141, neil.cameron@jci.com, www.johnsoncontrols.com
HID Global’s top trends for 2017

Increased adoption of mobile devices and the latest smart card technology.

HID Global forecasts a shift in the use of identity technology that will lead to increased adoption of mobile devices and the latest smart card technology, a greater emphasis and reliance on the cloud, and a radical new way of thinking of trust in smart environments and Internet of Things (IoT).

This shift will precipitate the move from legacy systems to NFC, Bluetooth Low Energy and advanced smart card technology to meet the evolving needs of organisations and governments worldwide. Ultimately, HID Global predicts the 2017 trends will transform the way trusted identities are used, particularly in industries focused on regulatory compliance, such as government, finance and healthcare markets.

Stefan Widing, president and CEO of HID Global says, “2017 will mark an important phase in the industry, as organisations seek to use the broadest range of smart devices than ever before. This will directly impact how customers view and use trusted identities on both mobile devices and smart cards.”

Mobile and smart cards

Similar to the adoption of consumer trends for IT in past years, 2017 will also see further consumerisation of security, with heightened demand from users seeking to open doors, and log in to cloud resources, as well as have personalised on-demand printing of documents, and to deploy printed credential remotely or conduct other transactions and daily activities using trusted IDs on their phone, wearable or smart card.

- Trusted IDs that integrate security, privacy and convenience will provide a new level of assurance to these applications and transactions, while being uniquely positioned to make secure access more personalised to the individual.
- The industry will look towards complete identity relationship management that considers the need to grant access based on the context or circumstances for risk appropriate authentication across trusted identities assigned to people, devices and things in smart offices, buildings and other environments that are becoming more connected every day.

HID Global anticipates the shift in the use of identity technology will drive industry trends in 2017, along with new solutions and capabilities that enhance the user experience for years to come.

For more information contact HID Global, +27 (0)83 321 2922, clangley@hidglobal.com, www.hidglobal.com

Surveillance trends for 2017

By Johan Crause, regional manager, Africa, Arecont Vision.

A different approach can improve security surveillance without increasing costs.

The rise of a depressed economy, particularly in South Africa, has caused a significant amount of pressure on most manufacturing concerns. The reality that security gets pushed to the doldrums infiltrates most businesses as most folk place emphasis on more pressing matters, such as paying salaries and keeping the proverbial lights on.

That being said, the security industry has an incredible way of re-inventing itself. With the advent of megapixel technology it has become evident that the ‘camera footprint’ is in danger of decreasing. Not only is this great news for our consumers, but it does question our intention with design. From a systems integrator perspective, are we actually after creating a monster amount of cameras or are we after minimising and more importantly optimising sites to assure client satisfaction?

A different approach

The answer is multi faceted. We as designers can get extremely lazy and stuck in a rut in the way that we have always done things, or we can invent a new approach to the problem by asking the correct questions and by utilising devices that are much smarter.

The use of multi-directional cameras placed in one housing is an example of how to decrease counts of cameras. Utilising high megapixel panoramic cameras is another.

Most of my learned friends would argue bandwidth, they would argue space and they would argue cost. Surprisingly on all three counts the manufacturers have come up with answers to our question. The invention of smart H.264 decreases a significant output of bandwidth to a minuscule amount, the driving down of price has made these products affordable. Understanding pixel density and how to optimise a design is of crucial importance and this will be a driving trend in 2017.

For more information contact Arecont Vision, +27 (0)82 553 9338, jcrause@arecontvision.com, www.arecontvision.com
Dealing with the insider threat

Teramind offers a range of solutions to combat the insider threat.

The threats to businesses from insiders cover areas such as malware deployment, but also fraud and sharing of company data with unauthorised third parties. When looking at insider incidents, research company Gartner says about 62% of these involve employees looking to establish a second stream of income from their employer’s data, while 29% steal information when they leave to help them in the future. Only 9% are saboteurs.

Protecting your business from threats like these, even simply preventing someone from taking a customer contact list, is not that easy in an environment where data is freely available. Employees often have customer lists, business plans and other sensitive data on mobile devices – laptops, tablets and smartphones – which is reasonable as it can assist them in making sales and servicing customers. But how does a business ensure this data does not end up supporting a competitor’s organisation?

Teramind has developed a range of solutions to combat the insider threat. The solutions are available either as a hosted or on-site system, where employees and data are automatically monitored. The cloud and on-site systems function identically. Moreover, the company is also pushing out a series of behavioural analytics that can identify suspicious behaviours and raise an alert, or even lock down the suspected user.

The employee-monitoring solutions are installed on users’ computers and monitor everything they do, from application usage through to email, even including web-based email offerings like Gmail. Management is able to draw reports and trends of behaviour, while ensuring that specific data is not sent out of the company.

Teramind’s behaviour monitoring application is able to create a baseline of acceptable behaviour for users, highlighting any anomalies and reacting in accordance with company policy – which could allow manual or automatic lock down in extreme cases. This year will also see the company releasing departmental monitoring, which monitors standard behaviours in departments, again reacting to anomalies as prescribed in the client’s policy.

Administrators are also able to customise their monitoring applications, to exclude Gmail from the monitoring process, for example.

The company is running a pilot site in South Africa and is expanding its reach in the region. Currently, local companies offering the Teramind solution include Telecommunications Solutions (crispin@telecommunicationsolutions.co.za) and infoGuardian (dylan@infoguardian.com)
Protection from ransomware

By Paul Williams, country manager – SADC at Fortinet.

10 steps for ransomware protection.

If you’ve been listening to the news in the past few months, you have undoubtedly heard of a number of companies being affected by ransomware. The recent surge in this form of cyber attack has many organisations and users understandably concerned. And you should be too.

Ransomware is nasty stuff. However, with some careful preparation, you can significantly lower your risk of being infected, and reduce the impact on you or your organisation should you be hit.

Ransomware is a form of malware that infects devices, networks and data centres, encrypting critical files and prevents them from being used until the user or organisation pays a ransom to have the system unlocked. Ransomware has been around since at least 1989, when the 'PC Cyborg' trojan encrypted file names on a hard drive and insisted users pay $189 to have them unlocked. In the interim, ransomware attacks have become increasingly sophisticated, targeted, and lucrative.

The impact of ransomware is difficult to calculate, since many organisations opt to simply pay to have their files unlocked – an approach that doesn’t always work. However, a report on the Cryptowall v3 ransomware campaign, issued in October of 2015 by the Cyber Threat Alliance, estimated that the cost of that attack was US$ 325 million.

Ransomware generally works in one of several ways. Crypto Ransomware can infect an operating system so that a device is unable to boot. Other ransomware will encrypt a drive or a set of files or file names. Some malicious versions have a timer and begin deleting files or a set of files or file names. Some malicious versions have a timer and begin deleting files until a ransom has been paid. All demand that a ransom be paid in order to unlock or release the blocked or encrypted system, files, or data.

What do I do to stop it?

Here are 10 things you need to do to protect yourself and your organisation from the effects of ransomware.

1. Develop a backup and recovery plan. Back up your systems regularly, and store that backup offline on a separate device.
2. Use professional email and web security tools that analyse email attachments, websites, and files for malware, and can block potentially compromised advertisements.
3. Keep your operating systems, devices, and antivirus, IPS, and antimalware tools running the latest updates.
4. Make sure that your device and network operating systems, devices, and software are patched and updated.
5. Where possible, use application white listing, which prevents unauthorised applications from being downloaded or run.
6. Segment your network into security zones, so that an infection in one area cannot easily spread to another.
7. Establish and enforce permission and privilege, so that the fewest number of users have the potential to infect business-critical applications, data, or services.
8. Establish and enforce a BYOD security policy which can inspect and block devices which do not meet your standards for security (no client or anti-malware installed, antivirus files are out of date, operating systems need critical patches, etc.).
9. Deploy forensic analysis tools so that after an attack you can identify:
   a) Where the infection came from,
   b) How long it has been in your environment,
   c) That you have removed all of it from every device, and
   d) That you can ensure it doesn’t come back.
10. This is critical: Do not count on your employees to keep you safe. While it is still important to increase your user-awareness training so employees are taught to not download files, click on email attachments, or follow unsolicited web links in emails, human beings are the most vulnerable link in your security chain, and you need to plan around them.

Here’s why: For many of your employees, clicking on attachments and searching the Internet is part of their job. It is difficult to maintain the appropriate level of scepticism. Second, phishing attacks have become very convincing. A targeted phishing attack uses things like online data and social media profiles to customise an approach. Third, it is simply human nature to click on an unexpected invoice or critical message from your bank. And finally, in survey after survey, users feel that security is someone else’s job, not theirs.

What if I get infected?

I hope that you have a recent backup and you can wipe your device and reload it with an uninfected version. Here are some other things you need to do:

1. Report the crime.
2. Paying the ransom is no guarantee.
3. Contact experts.
4. Have a Plan B.

“Ransomware is a form of malware that infects devices, networks and data centres, encrypting critical files and prevents them from being used until the user or organisation pays a ransom to have the system unlocked.”

Paul Williams, country manager – SADC at Fortinet.
Defining African communications

by Andrew Seldon.


The end of 2016 saw the latest AfricaCom exhibition happening in Cape Town. Hi-Tech Security Solutions was present at the event to witness the vast resources being poured into improving the communications capabilities of the continent, from the growth of fibre, satellite and a host of other options. Below are a few of the companies we met.

One of the companies at the event was Liquid Telecom, which is focusing on fibre communications – it was recently given the go-ahead to acquire Neotel. The company has a fibre network into numerous African countries, offering communications services to businesses with interests in the region. Its goal is to cover the continent and then expand its service offerings in different countries, such as it is doing with Neotel.

Liquid Telecom focuses on under-served countries where it can take the lead and develop a good business – such as its activities in the DRC, for example.

It’s the insides that count

Qualcomm is a company that has been in the technology space for many years. As far as communications in Africa is concerned, the company is focused on 4G and the eventual migration to 5G technologies. It not only provides the communications solutions in partnership with companies such as Ericsson, but the two have developed 4G solutions that cover a smaller area but offer more bandwidth, which would be appropriate for business parks or safe/smart city projects and even Internet of Things (IoT) solutions. The ability to manage these cells efficiently to ensure optimal resource utilisation is also a focus area.

Looking ahead, Qualcomm provides the internal components of many mobile devices today, and is working with the global brands (such as smartphone manufacturers, for example) to create home and business solutions as well as ‘next-generation’ products such as wireless chargers and facilitating the faster charging of devices.

The company also demonstrated augmented reality and virtual reality solutions that its technology enables. These technologies, once they become more affordable to the consumer, will change the way we interact with data of all sorts, enhancing and expanding our world dramatically.

The end of cables?

Two wireless networking companies Hi-Tech Security Solutions spoke to were also focusing on Africa and its lack of physical infrastructure, working to make communications solutions available to all without the need for cables.

Nick Watson, VP of EMEA, Ruckus Wireless, says the company has focused on making wireless internet access easier and available over a wider area than ever before. As an example, he notes that a safe/smart city will save significant costs if it is run over a Wi-Fi mesh rather than LTE or 5G. Ruckus makes it possible to create such a mesh of access points, with only one point linked to a fibre or microwave connection for access to the rest of the world (if required), that deliver the performance required – whether it’s free Wi-Fi in a city or video surveillance over wireless.

He noted that an efficient wireless network is not simply a factor of having a large bandwidth capacity, but depends on the design and products used to deliver the required performance. This would include the management software required to, for example, reroute traffic to avoid bottlenecks.

As always, when it comes to any communications and especially wireless, security is very important and Ruckus includes access authentication in its management of wireless systems.

Radwin was also at the event. It used the occasion to launch its latest Jet Air wireless communications solution for the residential market. The Jet Air PtMP series includes a base station that delivers 250 Mbps (or up to 750 Mbps) and is built on Radwin’s bi-directional Beamforming technology which has been adopted by tier-1 carriers worldwide. Jet Air enables service providers to deliver bandwidth-demanding services such as TV streaming, gaming and online applications for consumers without having to install cables.

As part of the new offering, the company is releasing two new subscriber units (SUs) that provide up to 100 Mbps: SU AIR for residential users and SU PRO for hybrid enterprise and residential segments. The new IP67 SUs support up to 256 QAM and are powered by the WINTouch application tool that automates installation and alignment to significantly shorten the installation process. A TurboGain slide-on antenna that doubles the service range is available with the new SUs.

Digital security

Gemalto, a digital security company, was also on the floor talking about its various security solutions for the finance, government and telco industries, as well as specific mobile security solutions. The company’s Neil Cosser is based in South Africa and operates throughout Africa. He noted that Gemalto offers solutions that secure enterprise data centres down to individual products such as mobile phones.

Cosser’s focus is on spreading the word on Gemalto’s encryption and authentication solutions, which have been adopted in a variety of organisations worldwide, and in Africa. It also offers secure appliances that only allow authorised users to access and decrypt data on the system – a form of encryption in a box. He says these devices are designed for performance and offer 100 000 encryption/decryption operations per second and are therefore enterprise ready.

Cosser finds African organisations are more aware than ever when it comes to security and are more willing to engage in discussions on the topic to find solutions pertinent to their needs. South African organisations are taking a hard look at data security this year to deal with PoP1, King IV and the new PCI DSS v3.

In the consumer space, Gemalto recently commissioned a study of over 1300 adult smartphone users across six markets, including South Africa, asking people about their mobile behaviour and security expectations.

The study showed that consumers are spending more time with their devices than ever before, over three hours a day on their smartphones and 87% of this time will be spent using apps. South African consumers tapping into mobile banking are also increasing, with 65.1% of them using their phones to access their bank accounts. “These figures demonstrate the increasing importance of mobile device security,” says Sherry Zameer, senior vice president for Africa at Gemalto.

Convenience and speed are also very important, valued by just under half (48%) of respondents. “This shows that while security is vital, people expect a frictionless experience. Industries and those in government designing apps for their own users should take note of this and ensure their software is lean, runs quickly, but is also fundamentally secure,” commented Zameer.

www.securitysa.com  February 2017  65
New surveillance solutions

By Andrew Seldon.

The start of 2017 sees the introduction of a new range of surveillance products and solutions into South Africa.

The Kedacom brand is well known in the East where it is a favourite with law enforcement, emergency services and public security sectors. The police in China and Singapore are users, as are emergency services in multiple provinces in South Korea, for example.

While the Kedacom range has a variety of products available, business development manager, Gino de Oliveira says the company focuses on delivering integrated solutions to a host of verticals. These include the mobile, portable, commercial, prisons, hospitals, traffic and safe city markets.

When it comes to mobile solutions, Kedacom has a full solution for service vehicles, from police or emergency and public security, through to public transport and logistics customers. The vehicle-mounted products are shockproof, easy to install and IP66 rated, meaning they are water and dust resistant.

A 360-degree PTZ camera has a magnetic base, for example, and is secured to a vehicle via five magnets and provides a clear image at speeds of up to 80 km/h. It also sports a 60 m embedded infrared (IR) capability and an eight-hour battery life. With Wi-Fi built-in, the system is simple to install and use, and data collected is transferred to the central command centre seamlessly when the vehicle is in Wi-Fi range (unless cellular connectivity is used). The PTZ delivers 1080p resolution at 30 frames per second (fps).

A second 360-degree PTZ is roof mounted and provides 20X or 33X optical zoom capability (depending on the model chosen). It offers IR illumination of up to 200 metres at night and is IP66 rated. This PTZ also delivers 1080P resolution at 30 frames per second. Additional cameras have and are being designed for in-vehicle surveillance.

Kedacom also makes its own modular in-vehicle network video recorders (NVRs) which are also shock proof and can support up to 4 TB in solid-state drives (SSD) or traditional 2.5-inch hard drives. The NVRs can provide Power over Ethernet (PoE) power to the cameras and support Wi-Fi to upload data to the central server when in range. They can also be equipped with two 3G or 4G SIM card slots.

A tablet computer or Control Pad is also available to allow the occupants to control the cameras while on the road for extended mobile functionality.

Portable solutions

Kedacom also develops body-worn solutions. These range from the body-worn camera, ear-hook and button cameras, through to body-worn devices such as the body-worn surveillance phone along with the required accessories. The cameras can be linked to a central command and control centre via 3G /4G or Wi-Fi wireless networks.

Kedacom has included a removable battery, GPS tracking and an SD card slot for storage with 32 GB standard, expandable to 128 GB. Two-way audio is enabled for communications between the user and his/her peers and the command and control centre.

The body-worn cameras have a smart docking station available from where the device can be charged and onboard data transmitted to Central Management Server (CMS) at the control centre. If required, each user can be issued with a PIN, which is entered into the device to either release the device at the start of a shift, or book it back in at the end of the shift. The docking station has three hard drive slots which support up to 6 TB per slot.

Recognitive technology

Kedacom also offers a range of IP cameras and storage with a host of analytical applications under its Recognitive branding, as well as its own command and control software for managing surveillance operations using a computer connected to the video management system (VMS).

The Recognitive technology can distinguish between people and cars and determine their key characteristics such as colour, speed and direction of movement. The details can be live viewed or archived for further analysis. For example, operating admin can take a snapshot of a person and track his or her activities in real time, or search it from stored video. Facial recognition technology is also available, but is currently undergoing testing for South African conditions.

Kedacom also offers a video synopsis application which condenses the video footage of hours or days into a few minutes. Within the synopsis, users can specify parameters to include in the condensed footage, such as cars, bicycles or people only, as well as specifying direction and colour as well.

Commercial

In the commercial range, Kedacom offers a range of IP cameras and NVRs, as well as 11 analytics applications that run on the edge, in other words, on the camera. The analytics include Guard Line (line crossing), Area Enter/Exit, Tampering, Defocus, Scene Change, Object Left/Removed, Motion Detection, Gathering (crowds gathering) and Audio Surge (changes in the audio levels).

Of particular interest in this range of cameras are the laser PTZs (using a laser beam instead of IR lights). One model provides for clear images at 2 km in the day and 1 km at night. The laser technology allows users to observe objects after dark at this distance. A larger PTZ offers the same quality, but can deliver images at 10 km in the day and 5 km at night with 60X optical zoom. Kedacom’s Starlight technology allows colour pictures to be viewed in conditions close to near total darkness.

The systems are ONVIF compliant and integration into Milestone, NUUO, Genetec and Geutebrück is in progress to allow companies to retain their existing surveillance products when using Kedacom technology.

The VMS supports full RAID storage as well as the KFS file system for more efficient storage of video. It also offers redundancy and automated failover solutions. Kedacom also offers storage solutions, such as its IP SAN storage area network that integrates seamlessly with the company’s VMS and can even be used as a slave if required. The top-tier hardware NVRs can handle up to 5000 channels, while the software NVRs can handle up to 500 000 channels.

Kedacom also provides an SDK for Linux, Windows, Android and iOS. When purchasing the company’s products, customers pay a once-off licence fee with no renewals. Any firmware upgrades are also provided on a complimentary basis. Kedacom will begin shipments to South Africa in 2017 and will have a stock holding in the country. De Oliveira says a demonstration area will also be opening in Fourways where customers will be able to see the various solutions in action.

As of January 2017, the product will be distributed by ADI Global, Elvey Security, EuroByte Technologies and PinnSec.

For more information, contact Gino de Oliviera, Forbatt SA, +27 (0)11 469 3598, forbattsa@yahoo.com.tw
ISS releases SecurOS 9.0

By Andrew Seldon.

New analytics included in latest VMS from Intelligent Security Systems (ISS).

Intelligent Security Systems (ISS) has announced the release of its new video management system (VMS), SecurOS 9.0. The system has been updated with a host of new features, including various add-ons for video analytics.

According to Eugene Kayat, MD of ISS Africa, SecurOS has been designed to support surveillance systems from small shops and businesses through to the largest enterprises and even city surveillance projects.

As a software company, ISS ensures that its VMS can easily integrate with almost any third-party solutions. The company has a team of developers constantly developing new integration software for products, and third parties are able to access the SecurOS software development kit (SDK) to develop their own integrations.

In addition to the core VMS, add-ons such as facial recognition, automatic number plate recognition, traffic monitoring, container recognition and more can be added to the system, depending on the customer’s needs. One of the benefits of purchasing SecurOS, according to Kayat, is that ISS only charges a once-off licence fee.

New features

Of the various new features in SecurOS 9.0, Kayat highlighted a few that are worth noting.

First, the new Computer Vision subsystem supports a variety of video analytics modules, including the ones designed to increase the situational awareness of SecurOS operators. This currently includes the Tracking Kit III plug-in, which offers:

- Crowd Detector – designed to detect potentially dangerous groups of people.
- Object Left Behind Detector – designed to detect abandoned objects.
- Intrusion Detector – designed to detect objects entering a forbidden area (crossing forbidden zone border).
- Loitering Detector – designed to detect people loitering and moving in the same area for some time.
- Running Detector – designed to detect people who move faster than is considered normal.
- Object Counter – designed to count objects (people, vehicles) crossing a line in each direction.

The new Emergency Service module reports incidents detected by SecurOS to external emergency service centres. When an incident occurs, the operator creates a report by completing the Emergency Ticket form. This includes the address, time and type of incident, and the operator can add comments if necessary. The ticket is then transferred as a package of metadata, which includes URLs to access the SecurOS video archive from an external monitoring centre.

The SecurOS media client also allows operators to save bookmarks to the video archive when an incident or even a suspicious activity occurs. Bookmarks can be added to a single frame or to an archive interval. Users can also search for bookmarks and alarms in the archive, filtering by time range, camera ID etc.

To improve the quality of live monitoring in situations where the network is poor or congested, the viewing frames per second (fps) can be set to a maximum. In addition, the native Dewarper has been updated and is now calibrated for most major fisheye/360-degree cameras. The following camera models have been added in this release: OnCam EVO-05-xxx, OnCam EVO-12-xxx, Hikvision DS-2CD6362F-xxx4, and Mobotix Q24M-Secure. Kayat says more cameras will be added in future updates – ISS sends out updates every four months.

The Event Viewer GUI has also been updated and now allows operators to switch between two operation modes: Monitoring mode (which shows live events) or Event Search mode (which allows users to search for events in a log). The Event Viewer is more interactive, with existing right-click controls to view event video in the media client, send a ticket to emergency services, and an upcoming feature to acknowledge alarms.

In addition, ISS is empowering Android smartphones or tablets to support the security operation, not only with the ability to view video, but as an additional sensor. For automatic number plate recognition, for example, the app allows users to take a picture of a number plate via their Android device, from where it can be compared to a database of suspicious vehicles. In future, this will be expanded to include facial recognition.

ISS has over 100 000 deployments of its technology in 53 countries. The products are implemented in banks, office, industrial and manufacturing sites, retail locations, petrochemical processing facilities, casinos, hospitals, schools etc. ISS Africa is responsible for sales and support to the African continent.

For more information contact ISS Africa,
+27 (0)83 330 8767, eugene.kayat@isscctv.com
Multi-lens panoramic camera

Dahua Technology has introduced its multi-lens 180° panoramic network IR bullet camera. The IPC-PFW8601-A180 provides added flexibility for capturing wide-area video surveillance. With real-time image splicing technology, the camera has three 2-MP sensors working in tandem to create a comprehensive 180° view. This camera replaces multiple single-sensor cameras to lower cost of installation, storage and maintenance.

Adjustments can be made to each sensor on contrast and brightness to achieve a clear panorama view. The multi-lens camera supports day/night mechanical IR cut filter and true WDR (120 dB) which makes it ideal for applications in fluctuating lighting conditions. In addition, this camera deploys Dahua Starlight Technology to deliver usable video with minimal ambient light.

The camera is equipped with a built-in intelligent video analytic algorithm, which can realise functions like tripwire, intrusion, abandoned object and missing object, to accurately respond to events in a specific area. At the same time, the camera features face detection and intelligent tamper detection, which means more efficient security surveillance.

The camera has smart IR technology which can adjust the intensity of the camera’s infrared LEDs to compensate for the distance of an object. Smart IR technology prevents IR LEDs from whitening out images as they come closer to the camera.

With an operating ambient temperature range of -40°C to +60°C, IP67 and IK10 rating, this camera suits almost any outdoor applications including open and expansive areas like borders, coastlines, highways, squares and stadiums.

For more information, contact Dahua Technology, +86 571 8768 8883, overseas@dahuatech.com, www.dahuasecurity.com

Multi-sensor vandal dome

VIVOTEK has introduced the new vandal dome, MS8392-EV, to upgrade its multiple-sensor product line. Building on the achievements of the MS8391-EV outdoor camera, the new MS8392-EV provides an all-in-one solution, featuring four 3-megapixel CMOS sensors with 180-degree panoramic views within a brand new aesthetic design.

For wide open areas requiring detailed coverage, such as parking lots, shopping malls, schools, parks and plazas, it can maximise the field of view and reduces the total number of cameras required, thereby saving on both installation time and maintenance costs. Specially equipped with a video alignment feature, the MS8392-EV allows users to optimise the image quality of each sensor and experience both natural and optimal continuous panoramic views. It is also equipped with a removable IR-cut filter and WDR enhanced technology to deliver day-and-night protection and extend image visibility under high-contrast lighting conditions.

Thanks to the robust protection of its IK10 and IP66-rated housing and its -50°C to 50°C wide temperature range, the MS8392-EV is able to withstand rain and dust and is safeguarded against vandalism and tampering when deployed for outdoor surveillance.

To eliminate interference caused by direct sunlight, the camera includes a sunshield for wall-mount applications, and users are free to choose either corner mount or pole mount accessories to achieve easy installation whatever the application is.

For more information contact VIVOTEK, +886 2 8245 5282, pr@vivotek.com, www.vivotek.com

MegaDome 4K dome camera

The 8-megapixel/1080p MegaDome 4K dual mode network camera is the new generation of Arecont Vision’s line of H.264 MegaDome cameras. This fully compliant implementation of H.264 (MPEG-4, Part 10) provides full 3840 x 2160 megapixel resolution at full video frame rates of 30 frames per second (fps) at 8-megapixel and 60fps in 1080p binning mode.

The MegaDome 4K provides an all-in-one solution with integrated 12-megapixel day/night camera, remote focus, remote zoom, P-iris, 4.4-10 mm lens, SDHC card, IP66 water/dust ingress rating and a vandal-resistant dome enclosure with IK-10 rating that features an installer-friendly design. With the features of SNAPstream to reduce bandwidth without impacting image quality, scaling, binning mode, privacy masking, extended motion detection and flexible cropping, the MegaDome 4K is a high sensitivity, Power over Ethernet (PoE - IEEE 802.3af) compliant camera.

Built with Arecont Vision's massively-parallel MegaVideo processing technology, this camera offers more than 27 times the resolution of standard resolution IP cameras with the ability to output full real-time frame rates and deliver high-quality megapixel imaging for both indoor and outdoor applications.

For more information contact Arecont Vision, +27 (0)82 553 9338, jcruse@arecontvision.com, www.arecontvision.com
Integration is the key to success

Customers are looking for solutions that exceed requirements and contribute to the bottom line.

Nowadays, no business would ever consider employing under-performing staff or implementing systems that simply meet requirements. Increasingly, customers are looking for solutions that exceed requirements and contribute to the bottom line.

G4S Electronic Specialised Solutions (ESS) is continually researching, sourcing, and in many instances developing technology that will add value to its customers. Due to the specialised nature of this business, and in line with G4S South Africa expanding the system integration business of its portfolio to enterprise-level integration, Tim Timmins has been appointed as head of technology.

Timmins has been in South Africa for the past 22 years, but hails from the building systems market in the UK and brings with him a total of 30 years’ experience in consultancy, integration and the distribution sides of the security industry.

Timmins explains why integration is key: “By implementing integration software, we are able to connect and control multiple devices to create an end-to-end security solution. However, the power of these systems in truly realised through video, image and data analytics software. Through constant automated digital screening and filtering, video analytics can identify and notify operators of potential issues. This together with the capability of pooling and synthesising large volumes of data allows business owners and security personnel to make quick, informed decisions.”

G4S ESS employs over 60 technical specialists who provide solution-driven systems ranging from CCTV, time and attendance, access control including evacuation, public address and fire detection and gas suppression. Its sector approach allows it to tailor solutions for each customer, but more importantly, to integrate these systems with each other as well as with customers’ existing enterprise relationship platforms.

The G4S Electronic Specialised Solutions’ service offering includes:

- **CCTV systems**: Following years of research and development, G4S is able to offer consumer and commercial customers a range of G4S designed and manufactured CCTV products. Its own CCTV range is designed and manufactured to international standards, however, G4S is technology agnostic and capable of recommending other products, depending on a customer’s specific requirements.

- **Advanced access control systems**: Access control installation is an essential component of a good security management system (SMS). It determines who enters the area, how the access is controlled and what technology or equipment is used to do the task. The access control system also supports the rest of the SMS, such as patrols, monitoring and reaction alarms.

  Access control is most efficient when introduced as part of a multi-layered defence and can be integrated with other core security aspects to create a seamless solution to protect your staff, buildings and assets, while helping you to save time and reduce administration overheads.

- **Alarm management**: The alarm management features of the G4S SMS enables security officers or other personnel to view, acknowledge and respond to alarms, such as a door being forced open, an alarm sensor being triggered, or a card reader being used at an unauthorised time.

  **Physical security information management (PSIM)**: G4S’s PSIM system provides building managers and company employees with a range of intuitive tools to support the management of a site and the day-to-day processes within it. Information captured and managed within the system can be ana-lyzed and used to generate reports, business intelligence and personal action plans. Automated reminders, action escalations and management information can be created and communicated easily and effectively.

- **Fire solutions**: G4S offers an extensive range of fire protection and safety systems and specialises in providing a pro-active approach to customer care in all aspects of fire and safety. It specialises in fire alarm systems, fire suppression systems and emergency lighting systems, all of which can be monitored by its 24/7 National Control Centre.

  G4S has identified the potential for growth in this area and has recently appointed Clinton Hodgson as business development manager for fire solutions to strengthen this division. Clinton has been involved in the fire and security industry in South Africa for the past 20 years. He has vast experience in the design and installation of fire safety systems and has advised many blue chip multi-nationals in this regard.

- **Time and attendance systems**: With a dedicated in-house research and development department, G4S provides complete on- and off-site software support to more than 80 customers in a broad range of business sectors. The G4S time and attendance solutions are reliable and user friendly and can be adapted with relative ease and at a low cost, which allows the company to accurately meet the exact requirements of its customers.

  **Perimeter protection**: G4S offers a comprehensive range of products and applications to enhance perimeter protection. The company’s teams are able to provide valuable advice to ensure that a fitting and cost-effective solution is designed.

For more information contact G4S Electronic Specialised Solutions, +27 (0)10 001 4500, tim.timmins@za.g4s.com, www.g4s.co.za
Access with Axxess

Axxess-E’s wireless access control solution saves time and cost of installations.

Creating a business environment geared around ease-of-use, reliability and cost-effectiveness is a primary driver for MiRO. The recent addition of the Axxess-E range of wireless access control solutions to its portfolio is clearly underpinned by the company’s vision of creating increased return on investment for its customers.

Garth Baird, CEO of Optimised Axxess, says that the development team responsible for Axxess-E leveraged their 20-plus years in access control system development and support to identify and address issues related to hardwired access control systems.

“Some of the challenges faced by customers include bad connection procedures during installation and use of inferior or incorrect cables, which both lead to an unstable system. It is challenging to do fault-finding when something goes wrong down the line with larger hardwired systems. Complexity increases proportionately with the size of the installation. “The idea behind the development of Axxess-E was to speed up installation times and simplify the installation. Installers can complete projects much faster, which enables them to take on more projects with the same labour force. Simpler installations minimise the cost of maintenance and reduce the aggravation that customers experience when trying to effectively undertake fault-finding,” he continues.

Site problems are often caused by third-party contractors who move into a site to perform work that is not related to the access control system. Cabling can be cut or be partially damaged, a situation that leads to intermittent faults.

Apart from reduced installation time and cost savings, Axxess-E wireless access control solutions provide customers with a number of other benefits. The intelligent transmission, with Clear Channel Assessment, means that data crashing is avoided, since devices only transmit when the channel is clear. The ease-to-use software development kit enables customers to integrate the Axxess-E hardware into their own software or management system to expand the functionality of their system. Using a Wiegand interface, the software seamlessly integrates with well-known biometric readers for full wireless functionality.

“We anticipate a mindset change from installers when they weigh up the advantages of wireless over hardwired access control systems. By reducing the installation time required, installers will be able to increase their workload and turnover. Together with our own technical team, MiRO will provide a large platform from which we will be able to both advise customers on best fit and provide extensive support for the Axxess-E range,” says Baird.

For more information contact MiRO Distribution, 086 123 MIRO, lerize@miro.co.za, www.miro.co.za

Gallagher releases mobile security

Smartphones become your access credentials.

Gallagher has announced the global release of its latest mobile security solution: Gallagher Mobile Connect. Harnessing Bluetooth wireless technology and the power of smartphones, Mobile Connect transforms a mobile phone into an access device – empowering businesses to use mobile technology in place of traditional access cards. Partnering with Nok Nok Labs and the FIDO (Fast Identity Online) Alliance, Gallagher’s Mobile Connect uses FIDO-certified authentication to deliver exceptionally safe and secure credentials.

“Mobile Connect really brings the best of both worlds to the market,” said Steve Bell, chief technology officer at Gallagher. “It makes access simpler and easier for users while operating on highly-secure, cutting-edge FIDO protocols that give businesses supreme confidence in their security.”

Delivering more than just peace-of-mind, Gallagher’s new mobile solution significantly reduces costs and simplifies administration through a range of exclusive features. In addition to eliminating the costs of supplying and replacing access cards, Mobile Connect customers will enjoy a unique subscription model, which allows for credentials to be transferred between users and reissued to devices.

Using two-step remote provisioning, Mobile Connect delivers secure enrolment by sending an email invitation with SMS code to verify the user and mobile device. This creates further administration efficiencies by removing the need to physically deliver an access card.

Optional two-factor authentication, either PIN or biometric, provides added security and flexibility for sites using Mobile Connect.

“We’re thrilled with this latest release in our mobile technology development program and the simplicity it brings to our customers. Our goal is always to develop simple solutions underpinned by the strongest security, and that’s what we’ve achieved here,” said Bell.

For more information contact Gallagher Security, +27 (0)11 974 4740, sales.africa@security.gallagher.co, www.gallagher.co
New generation e-Gates in Christchurch

Morpho goes live with new SmartGate Plus in Christchurch Airport, New Zealand.

Safran Identity & Security, through its subsidiary, Morpho Australasia, has completed installing the next generation of e-Gates into Christchurch Airport. Traveller volumes in New Zealand are expected to increase by 4-5% annually, or around 2.3 million to nearly 12.7 million by 2019.

This installation is part of a national upgrade and innovation programme for 51 new generation border processing e-Gates for the New Zealand Customs Service (NZ Customs). The rollout has seen new generation Safran Identity & Security’s e-Gates installed in Auckland, Wellington, Queenstown and now Christchurch Airport.

Since 2009, Auckland, Wellington and Christchurch Airports have been using SmartGate to give eligible travellers the option of self-processing through passport control. The system uses facial recognition technology to compare facial images of the traveller against the data contained in the e-Passport’s chip. Over 18 million passengers have successfully used the system.

The new generation e-Gates speed up the traveller experience with a one-step process, eliminating the kiosk and ticket which was part of the process with the previous gates. They also have a smaller footprint to meet the space constraints of airports, while also having Safran Identity & Security’s latest workflow and biometric matching software.

“As a company, we are focused on providing NZ Customs with a range of innovative services and technologies to help with passenger flow. We are proud of our joint innovation journey and are looking forward to launching the next series of passenger technology to help NZ Customs continue as world leaders at the border.”

Carolyn Tremain, comptroller and chief executive of NZ Customs.

Tim Ferris, MD of Morpho Australasia, added: “As a company, we are focused on providing NZ Customs with a range of innovative services and technologies to help with passenger flow. We are proud of our joint innovation journey and are looking forward to launching the next series of passenger technology to help NZ Customs continue as world leaders at the border.”

For more information contact Morpho South Africa, +27 (0)11 286 5800, sec.san.morpho@morpho.com, www.morpho.com

Asset monitoring solution

FPX10 device adapted for office key audits.

The company charged with managing a newly completed office park required a facility capable of monitoring the whereabouts and movements of its office keys.

At the outset of its contract, management had installed FPX10 devices at the access points of every building, as well as in the central office. The rationale behind the installations was to monitor the performance and quality of services rendered by the park’s cleaning staff.

At the suggestion of Active Track – the FPX10 distributor – the FPX10 device in the central office was programmed to perform office key audits. Part of the programming involved attaching an RFID card to every office key, recording the RFID cards’ details, and capturing the fingerprints of all sales agents via the FPX10 scanner. The RFID card and fingerprint data was uploaded to the FPX10 online platform and stored in the cloud.

When a sales agent wished to check an office key in or out from the park’s central office, he/she would be required to scan his/her fingerprint, and the key’s RFID card, on the FPX10 reader.

Meanwhile, the employee on duty in the central office was obliged to scan the RFID tag of each key in its possession, every eight hours. If a key was not in the central office – that is, either having been checked out by a sales agent, or unaccounted for – an alert would be sent via SMS and/or email to the designated park manager, notifying him/her of the finding and details of the outstanding key. An alert would be similarly sent if the audit was not conducted, or was conducted late, thereby enabling management to take the appropriate remedial action.

In order for park management to reap the full benefit of the audit function, the FPX10 device was programmed to automatically generate daily, weekly and monthly reports from the data captured in the central office. These were made available, in real time, via the online portal.

This adaption of the FPX10 technology resulted in greater accountability and certainty among both park management and staff; and a reduction in the rate of lost keys, and exposure of office property to theft.

For more information contact Active Track, +27 (0)11 551 1687, info@activetrack.co.za, www.activetrack.co.za.
Mobile app and three modes of communication

The addition of the Permaconn range of wireless alarm communication products to Elvey’s portfolio underlines the company’s commitment to continually servicing market needs. Gary Lowe, CEO of Elvey, says that Permaconn’s 17-year track record in developed markets, coupled with the benefits that Permaconn’s range offers the market, makes this a welcome addition to Elvey’s suite brands and solutions.

Permaconn offers a clear set of differentiating factors from the existing GPRS transmitters available in South Africa. Not only does each transmitter come with a standard Ethernet connection, but one can also set various polling rates, based on a site’s security requirements. The Permaconn transmitters can operate on GPRS, 3G and IP networks. The system incorporates a primary IP link and will switch over to GPRS when required.

“Furthermore, it allows remote up and downloading capabilities on all of Elvey’s control panel options. Add to this the Pocket Secure mobile app that allows you to arm or disarm your alarm system, control doors, gates and lights,” says Elvey sales director, Ingo Mutinelli.

Mutinelli explains that Commercial ICT, the exclusive distributors of the Permaconn product range, concluded a deal with Elvey to simultaneously distribute the Permaconn brand. This arrangement leverages the technical skills, experience and expertise of both companies and increases the level of support available to customers.

This makes it an attractive option. Added to the obvious reliability of communication is the redundancy in the control room provided by the disaster recovery module (DRC). In essence, during evacuation situations in control room centres, a dongle plugged into a secondary station in a disaster recovery centre can be used to restore signals in real time. In addition, two data centres – one at MTN and one in Australia – provide redundancy should one network go offline.

The Permaconn products are compatible with many alarm manufacturer brands and have full RISCO congruity for complete video integration, making them cost-effective choices. Because all signals are encrypted via AES128, users have the peace of mind that they cannot be hacked. The units have a low current consumption, so in the event of a power failure, they will remain on line for longer.

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

Multi-biometric ID for Mexico

Safran Identity & Security to modernise Mexico’s multi-biometric identification system.

Safran Identity & Security has been awarded a five-year contract by the National Electoral Institute of Mexico (INE) for its multi-biometric identification system and related services. With this new contract, INE confirms its trust in Safran to conform and update the Mexican national voter registry that enables fair and efficient elections.

As one of the world’s largest systems of its kind, the multi-biometric identification system ensures each voter has a unique identity by detecting false or double-identity cases in real-time. It uses both fingerprint and facial recognition to help ensure that each Mexican citizen is registered only once in the national voter rolls.

Safran has supported INE with its multi-biometric system since 2005. The latest contract comprises the modernisation of the system with the latest biometric technology and an upgrade from 2 to 10 fingerprint matching. The new system will be able to register 113 million fingerprint captures and portrait images. These will be matched against the largest database in the region. Safran’s solution is designed to support up to 120 000 transactions per day.

“As an autonomous public entity responsible for organising federal elections, we need to ensure the trustworthiness of the process,” said René Miranda Jaimes, executive director of the Electoral Federal Registry at INE. “For more than 10 years, Safran has proven it fulfills this demanding requirement. By choosing the world leader in biometric technology, INE is making sure it is well prepared for the future with state of the art technology.”

For more information contact Morpho South Africa, +27 (0)11 286 5800, sec.san.morpho@morpho.com, www.morpho.com
Tyco Security Products introduced the new exacqVision M-Series, a cost-effective network video recorder which makes IP CCTV easy to install and easy to use. The exacqVision M-Series is perfect for surveillance systems needing up to 8 cameras; the integrated PoE ports, video management system and client are all contained within the 4 or 8 IP camera server, so no external and costly PoE switch is needed. There are no camera licences to purchase or apply as the M-Series is fully licensed out of the box, which adds to the ease of installation.

With up to 8 IP cameras per system, users can choose to view the live and recorded video in a way that best suits their needs. Both the on-board client and free remote client enables the user to administer their system as well as the video. For those who require the additional freedom of using a browser or app, the M-Series NVR can be accessed from any web browser and from the exacq Mobile App available for iOS and Android devices.

Like all exacqVision recording solutions, the M-Series is very easy to set up as the intrinsic exacqVision EasyConnect feature automatically finds, assigns and addresses Illustra and other brands of IP cameras to the network. This enables installers to take advantage of the plug-and-play system architecture of the M-Series, significantly reducing installation time and the need for an in-depth knowledge of IP.

For more information contact Tyco Security Products, +27 (0)82 566 5274, emallett@tycoint.com, www.tycosecurityproducts.com

New exacqVision M-Series
ZK introduces F22

The F22 is an ultra-thin fingerprint time, attendance and access control terminal with BioID sensor and Wi-Fi, that offers performance with an advanced algorithm for reliability, precision and excellent matching speed. The new terminal features the fastest commercial-based fingerprint matching algorithm and ZK’s high-performance, high-image quality infrared detection fingerprint sensor.

The F22 provides a superior touching experience with touch keypad, and offers flexibility for standalone installation or with any third-party access control panel that supports standard wiegand signals. TCP/IP, RS-485 and Wi-Fi are also available so that the device can be used in different networks.

Features
• 2.4-inch TFT colour screen and touch keys.
• Ultra thin design.
• Full access control features:
  o Anti-passback, access control interface for third-party electric lock, door sensor, exit button, alarm.
• Standard Wi-Fi.
• Network interface via TCP/IP or RS-485.
• Built-in auxiliary input with enhanced flexibility to link with wired detector or emergency switch.
• Multiple verification modes: multi-verification methods (card is optional) providing various user choices.

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

Smart power monitoring solutions

BT-SA has introduced a range of smart power monitoring solutions that could save households and companies money during power outages. This forms part of its strategy to create an overall Internet of Things (IoT) business environment.

Power trips, load shedding, storms, inadequate general maintenance and bad maintenance of poles are some of the reasons why power could go out and there are many reasons why monitoring power is a good idea.

The cloud or network-managed Smart Zero U Power Distribution Units (PDUs) provide active Class 1 metering, so that clients are able to take advantage of energy metering and energy optimisation of cabinets in their data centres. The units also offer the option to add temperature, humidity and fluid monitoring sensors.

BT-SA managing director, Bertie Strydom, says companies still face challenges with the management of effective power distribution, power protection and power management in their data centre cabinets. “Making use of one of these Smart PDUs will help companies better manage existing power capacity to improve data cabinet efficiency, uptime and expansion.”

The Smart PDUs provide users with remote power monitoring and rack sensor information regarding the conditions inside the data centre via a Web interface or SNMP managed by a centralised or cloud-based management system. This means businesses will be able to mitigate risks with user-definable alarms with real-time alerts, giving them control and keeping them in the know no matter where they are.

The units also provide remote monitoring of current, voltage, power, energy usage and environmental conditions, as a result users are warned of potential circuit overloads and nominal consumption increases. In addition they offer remote power switching for emergency shutdowns or to reboot hanging servers.

Simple single-phase GSM Power Monitor PH1

The new single-phase GSM Power Monitor PH1 presents a convenient remote power monitoring solution. The unit needs to simply be plugged into any power plug, a SIM card added, SMS the number that it needs to report to and the unit will then monitor the premises’ mains power and temperature.

Notifications about the status of power are sent straight to the user’s cellphone via SMS and the unit can send SMS-based status reports at the user’s request. In addition, the simple GSM Power Monitor has front-mounted LED indicators to show network and functional statuses.

Features of the unit also include an integrated South African three pin plug, utility mains power detector (single phase), GSM unit with a Micro SIM socket that is externally accessible, an internal GSM antenna, and an internal Lithium-ion polymer rechargeable backup battery and charger.

The unit can also be expanded to measure environmental temperature in a range from -45 to 145°C in one degree steps and also has optional connectivity to stream warnings through GPRS connectivity. Furthermore, the unit’s GSM capability has been ICASA approved.

For more information contact BT-SA, 0860 105 183, sales@bt-sa.co.za, www.bt-sa.co.za
4K IR fisheye cameras

Hanwha Techwin is launching a 9 megapixel 4K ultra-high-definition network IR Fisheye camera series. The fisheye cameras, PNF-9010R/9010RV, supporting 25fps at 9 megapixels and up to 20fps at 12 megapixels (4000x3000), provide very clear and detailed images for monitoring even when enlarged. As fisheye cameras, the new series offer 360° surround view, and with various view modes available, they can be used flexibly in many different surveillance environments.

Also, the Simple Focus function makes it very easy to adjust lenses for focus settings in the installed camera. This function is useful when the focus point of an outdoor camera is warping due to temperature difference, impact, or vibration. The focus can be finely tuned easily by using the Simple Focus button.

People counting and Heatmap functions allow users to analyse and optimise store layout in retail shops, etc., and provide useful information for analysis of store customers.

In addition, the built-in IR LED provides illumination up to 15 m under low-light situations, and with True WDR 120 dB and IP66/IK10 (PNF-9010RV/9010RVM), it delivers stable surveillance with clear images in any conditions, including backlight and any outdoor environment. Hanwha Techwin says that its new 4K IR Fisheye Camera Series PNF-9010R/9010RV/9010RVM enable ultra HD monitoring and efficient surveillance with a single camera, and can satisfy the customer’s needs in specific markets.

For more information contact Hanwha Techwin (formerly Samsung Techwin), Jaco De Wet, +27 (0)79 843 4051, jaco@stcctv.co.za

Control cables with numbered cores

Equipment and machinery installations using the latest cabling technologies can contribute significantly to the ease of installation and overall success of a project.

A good example of this is Helukabel’s JZ500 flexible control cable, which is designed to be supple, yet strong enough to be used in the toughest industrial conditions where its oil and chemical resistance makes it ideal for toolroom controls, conveyor applications, production lines, air condition and steel production among others.

Another unique feature is its easy-to-read core identification to DIN VDE 0293 that has black cores with continuous white numbering (also available in other colours on request) for ease of installation, particularly where long runs are required or individual installers are working at different ends. The numbering, colours and other special requirements can also be ordered to suit different applications.

According to Hardus van Dyk of Helukabel, the cables are designed for flexible use for applications requiring medium mechanical stresses with free movement – without tensile stress or forced movements and can be used in either dry, moist or wet rooms. Selected PVC-compounds guarantee a good flexibility as well as an economic and fast installation.

The materials used in manufacture are cadmium-free and contain no silicone and are free from substances harmful to the wetting properties of lacquers. The cable also conforms to relevant national and international standards and requirements.

For more information contact Helukabel SA, +27 (0)11 462 8752, doug.gunneweg@helukabel.co.za, www.helukabel.co.za.

8CH NVR with POE

The XRN-810S from Hanwha Techwin offers WiseStream support, which can reduce bandwidth and storage requirements of surveillance feeds by up to 75%. It supports H.265 / H.264/ MJPEG compression, as well as Automatic Recovery Backup for redundant recording.

Key features

• 8 megapixel supported
• H.265, H.264, MJPEG codec supported

WiseStream support
• 100 Mbps network camera recording
• Max. 2 HDDs, e-SATA storage supported
• HDMI/VGA local monitor

For more information contact Hanwha Techwin (formerly Samsung Techwin), Jaco De Wet, +27 (0)79 843 4051, jaco@stcctv.co.za
FLIR Systems announced the second generation of the FLIR Meridian Network Video Recorder (NVR). The Meridian NVR is a cost-effective, enterprise grade, off-the-shelf, plug-and-play video surveillance system for security installations, configurable for 8, 16 or 24 cameras. The system includes a network video recorder with a built-in 8-port PoE switch (additional 8-port PoE switch available for purchase), video management software that is pre-configured, support for the EZ Client web interface and works out-of-the-box with sophisticated viewing capabilities, eliminating the need for additional client workstations.

With new dual monitor support, users can easily control multiple cameras, quickly browse through recorded footage, and generate detailed reports using FLIR’s built-in United VMS Control Centre, or the modernised EZ Client web interface, which is optimised for touch-screen monitors.

VMS 7.0 reinvents the user experience with a new, sleek and efficient EZ Client web interface with responsive design, allowing for effortless deployment, touch-screen optimisation and support on multiple browsers.

For more information contact TeleEye (South Africa), +27 (0)11 557 9200, info@teleeye.co.za, www.teleeye.com

Second generation FLIR Meridian NVR

FLIR’s FC-Series ID thermal cameras

Graphic Image Technologies (GIT) has announced the local availability of the FC-Series ID thermal security cameras, the latest models in its FC-Series line. The FC-Series ID thermal cameras combine built-in analytics for high-performance intrusion detection, image quality designed for high-end commercial users and an expanded selection of high-performance lenses to suit a wide range of applications.

The FC-Series ID cameras see heat instead of light, and thus deliver superior image quality in what are typically considered challenging conditions for visible light or IR illuminated cameras. By seeing only thermal energy, the cameras see clearly in complete darkness, without any illumination and are immune to the effects of sunlight, shadows, smoke, haze, insects and even light fog.

In addition, the FC-Series ID cameras are available with a wide selection of high-performance lenses, ranging from wide angle to narrow fields of view, with either VGA or QVGA resolution. Combined with a choice of 320 or 640 resolutions, the FC-Series ID cameras offer more fields of view and resolution options than any other commercial thermal security camera line.

“Our new FLIR FC-Series ID cameras build upon the industry’s most popular thermal security camera line,” said John Distelzweig, vice president and general manager of FLIR’s security segment. “The new cameras offer security professionals the highest operational availability coupled with the lowest false alarm rates using the latest edge-based thermal video analytics.”

For more information contact Graphic Image Technologies, +27 (0)11 483 0333, laurence@git.co.za, www.git.co.za

Arecont Vision MegaVideo Flex

The MegaVideo Flex Series is a compact true day/night single-sensor all-in-one IP camera solution available in 1.2 MP, 1080p, 3 MP or 5 MP resolutions. This camera is designed to fit compact spaces where the constraints of ordinary cameras are a challenge. The simplicity of the design allows installers the flexibility of installing the camera in one area and hiding the main unit up to 12 m away. Additionally, light up the night by adding up to two external IR illuminators (sold separately).

For more information contact Arecont Vision, +27 (0)82 553 9338, jcruse@arecontvision.com, www.arecontvision.com
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>E-mail</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access and Beyond</td>
<td>+27 (0)31 263 1487</td>
<td><a href="mailto:info@accessandbeyond.com">info@accessandbeyond.com</a></td>
<td><a href="http://www.accessandbeyond.com">www.accessandbeyond.com</a></td>
<td>23*</td>
</tr>
<tr>
<td>Active Track</td>
<td>+27 (0)11 551 1687</td>
<td><a href="mailto:info@activetrack.co.za">info@activetrack.co.za</a></td>
<td><a href="http://www.activetrack.co.za">www.activetrack.co.za</a></td>
<td>71</td>
</tr>
<tr>
<td>Arecont Vision</td>
<td>+27 (0)82 553 9338</td>
<td><a href="mailto:jcrause@arecontvision.com">jcrause@arecontvision.com</a></td>
<td><a href="http://www.arecontvision.com">www.arecontvision.com</a></td>
<td>62,68,76</td>
</tr>
<tr>
<td>BT-SA</td>
<td>0860 105 183</td>
<td><a href="mailto:sales@bt-SA.co.za">sales@bt-SA.co.za</a></td>
<td><a href="http://www.bt-sa.co.za">www.bt-sa.co.za</a></td>
<td>74</td>
</tr>
<tr>
<td>Catheixs Africa</td>
<td>+27 (0)31 240 0800</td>
<td><a href="mailto:sales@catafrica.com">sales@catafrica.com</a></td>
<td><a href="http://www.catheixsvideo.com">www.catheixsvideo.com</a></td>
<td>29*,58</td>
</tr>
<tr>
<td>Dahua Technology</td>
<td>+26 571 8768 8883</td>
<td><a href="mailto:overseas@dahuatech.com">overseas@dahuatech.com</a></td>
<td><a href="http://www.dahauasecurity.com">www.dahauasecurity.com</a></td>
<td>3*,68</td>
</tr>
<tr>
<td>Dallmeier Southern Africa Office</td>
<td>+27 (0)11 510 0505</td>
<td><a href="mailto:dallmeiera@dallmeier.com">dallmeiera@dallmeier.com</a></td>
<td><a href="http://www.dallmeier.com">www.dallmeier.com</a></td>
<td>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>15*,72,73*</td>
</tr>
<tr>
<td>EOH</td>
<td>+27 (0)11 607 8346</td>
<td><a href="mailto:kedibone.sehume@eoh.co.za">kedibone.sehume@eoh.co.za</a></td>
<td><a href="http://www.eoh.co.za">www.eoh.co.za</a></td>
<td>22</td>
</tr>
<tr>
<td>Forbatts SA</td>
<td>+27 (0)11 469 3598</td>
<td><a href="mailto:forbatta@yaho.com.tw">forbatta@yaho.com.tw</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G4S Specialised Solutions</td>
<td>+27 (0)10 001 4500</td>
<td><a href="mailto:tim.timmins@africa.g4s.com">tim.timmins@africa.g4s.com</a></td>
<td><a href="http://www.g4s.co.za">www.g4s.co.za</a></td>
<td>69</td>
</tr>
<tr>
<td>Gallagher Security</td>
<td>+27 (0)11 974 4740</td>
<td><a href="mailto:sales.africa@security.gallagher.co">sales.africa@security.gallagher.co</a></td>
<td><a href="http://www.gallagher.co">www.gallagher.co</a></td>
<td>70</td>
</tr>
<tr>
<td>GateBook</td>
<td>+27 (0)31 035 0941</td>
<td><a href="mailto:info@gatebook.co.za">info@gatebook.co.za</a></td>
<td><a href="http://www.gatebook.co.za">www.gatebook.co.za</a></td>
<td>57*</td>
</tr>
<tr>
<td>GeoVision SA</td>
<td>+27 (0)12 664 0411</td>
<td><a href="mailto:sales@geovision.co.za">sales@geovision.co.za</a></td>
<td><a href="http://www.geovision.co.za">www.geovision.co.za</a></td>
<td>10</td>
</tr>
<tr>
<td>Graphic Image Technologies</td>
<td>+27 (0)11 483 0333</td>
<td><a href="mailto:laurence@git.co.za">laurence@git.co.za</a></td>
<td><a href="http://www.git.co.za">www.git.co.za</a></td>
<td>76</td>
</tr>
<tr>
<td>Hanwha Techwin</td>
<td>+27 (0)79 843 4051</td>
<td><a href="mailto:jaco@stcctv.co.za">jaco@stcctv.co.za</a></td>
<td><a href="http://security.hanwhatechn.com">http://security.hanwhatechn.com</a></td>
<td>75</td>
</tr>
<tr>
<td>(Formerly Samsung Techwin)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Helukabel South Africa</td>
<td>+27 (0)11 462 8752</td>
<td><a href="mailto:sales@helukabel.co.za">sales@helukabel.co.za</a></td>
<td><a href="http://www.helukabel.co.za">www.helukabel.co.za</a></td>
<td>63*,75</td>
</tr>
<tr>
<td>HID Global</td>
<td>+27 (0)83 321 2922</td>
<td><a href="mailto:clangley@hidglobal.com">clangley@hidglobal.com</a></td>
<td><a href="http://www.hidglobal.com">www.hidglobal.com</a></td>
<td>62</td>
</tr>
<tr>
<td>Hikvision South Africa</td>
<td>+27 (0)10 035 1172</td>
<td><a href="mailto:support.africa@hikvision.com">support.africa@hikvision.com</a></td>
<td><a href="http://www.hikvision.com">www.hikvision.com</a></td>
<td>IFC*,32</td>
</tr>
<tr>
<td>Hi-Tech Security Solutions</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>47*</td>
</tr>
<tr>
<td>Hochiki Europe</td>
<td>+41 1634 266 568</td>
<td><a href="mailto:padams@hochikiurope.com">padams@hochikiurope.com</a></td>
<td><a href="http://www.hochikiurope.com">www.hochikiurope.com</a></td>
<td>49*,52</td>
</tr>
<tr>
<td>Huawei</td>
<td>+27 (0)11 517 9800</td>
<td><a href="mailto:shonisani.mudau@huawei.com">shonisani.mudau@huawei.com</a></td>
<td><a href="http://www.huawei.com/enterprise">www.huawei.com/enterprise</a></td>
<td>21*,28</td>
</tr>
<tr>
<td>Impro Technologies</td>
<td>+27 (0)31 717 0700</td>
<td><a href="mailto:vikkiv@impro.net">vikkiv@impro.net</a></td>
<td><a href="http://www.impro.net">www.impro.net</a></td>
<td>10,42,43</td>
</tr>
<tr>
<td>ISS 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>67</td>
</tr>
<tr>
<td>Johnson Controls</td>
<td>+27 (0)11 921 7100</td>
<td><a href="mailto:neil.cameron@jci.co.za">neil.cameron@jci.co.za</a></td>
<td><a href="http://www.johnsoncontrols.com">www.johnsoncontrols.com</a></td>
<td>33*,61</td>
</tr>
<tr>
<td>Kifarun Management Services</td>
<td>+27 (0)72 596 2621</td>
<td><a href="mailto:chris@kifarumangement.co.za">chris@kifarumangement.co.za</a></td>
<td></td>
<td></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>14,15</td>
</tr>
<tr>
<td>MASS</td>
<td>+27 (0)12 142 0000</td>
<td><a href="mailto:info@mass-solutions.co.za">info@mass-solutions.co.za</a></td>
<td><a href="http://www.mass-solutions.co.za">www.mass-solutions.co.za</a></td>
<td>35*</td>
</tr>
<tr>
<td>MIA Telecoms Surveillance</td>
<td>+27 (0)11 799 7720</td>
<td><a href="mailto:michael@mia.co.za">michael@mia.co.za</a></td>
<td><a href="http://www.mia.co.za">www.mia.co.za</a></td>
<td>25*</td>
</tr>
<tr>
<td>MiRO distribution</td>
<td>086 123 MiRO (6476)</td>
<td><a href="mailto:lerize@miro.co.za">lerize@miro.co.za</a></td>
<td><a href="http://www.miro.co.za">www.miro.co.za</a></td>
<td>70</td>
</tr>
<tr>
<td>Morpho SA</td>
<td>+27 (0)11 286 5800</td>
<td><a href="mailto:sec.san.morpho@morpho.com">sec.san.morpho@morpho.com</a></td>
<td><a href="http://www.morpho.co.za">www.morpho.co.za</a></td>
<td>5*,71,72</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>61*</td>
</tr>
<tr>
<td>Paxton Access</td>
<td>+27 (0)21 427 6691</td>
<td><a href="mailto:support@paxtonaccess.co.za">support@paxtonaccess.co.za</a></td>
<td><a href="http://www.paxtonaccess.co.za">www.paxtonaccess.co.za</a></td>
<td>6</td>
</tr>
<tr>
<td>Powell Electronics</td>
<td>0861 787 2537</td>
<td><a href="mailto:marketing@powelltronics.com">marketing@powelltronics.com</a></td>
<td><a href="http://www.p-tron.com">www.p-tron.com</a></td>
<td>7,42,43*,47</td>
</tr>
<tr>
<td>Progroup Manufacturing</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>59*</td>
</tr>
<tr>
<td>Radwin</td>
<td>+27 (0)74 114 2805</td>
<td><a href="mailto:nick.ehrke@radwin.com">nick.ehrke@radwin.com</a></td>
<td><a href="http://www.radwin.com">www.radwin.com</a></td>
<td>33,34</td>
</tr>
<tr>
<td>Rob Anderson &amp; Associates</td>
<td>+27 (0)31 267 4150</td>
<td><a href="mailto:rob@robanderson.co.za">rob@robanderson.co.za</a></td>
<td><a href="http://www.robanderson.co.za">www.robanderson.co.za</a></td>
<td>8</td>
</tr>
<tr>
<td>Seagate South Africa</td>
<td>+27 (0)76 360 2850</td>
<td><a href="mailto:martin.kruger@seagate.com">martin.kruger@seagate.com</a></td>
<td><a href="http://www.seagate.com">www.seagate.com</a></td>
<td>27*</td>
</tr>
<tr>
<td>Securiton AG</td>
<td>+41 31 910 1398</td>
<td><a href="mailto:info@securiton.com">info@securiton.com</a></td>
<td><a href="http://www.securiton.com">www.securiton.com</a></td>
<td>7*,11*,52</td>
</tr>
<tr>
<td>Security &amp; Communication Warehouse</td>
<td>+27 (0)12 653 1005</td>
<td><a href="mailto:marketing@securitywarehouse.co.za">marketing@securitywarehouse.co.za</a></td>
<td><a href="http://www.securitywarehouse.co.za">www.securitywarehouse.co.za</a></td>
<td>54,56</td>
</tr>
<tr>
<td>SFP Security &amp; Fire</td>
<td>+27 (0)11 247 7800</td>
<td><a href="mailto:dan@sfp.co.za">dan@sfp.co.za</a></td>
<td><a href="http://www.sfp.co.za">www.sfp.co.za</a></td>
<td>48</td>
</tr>
<tr>
<td>Solution House</td>
<td>+27 (0)82 565 8081</td>
<td><a href="mailto:tian@solutionhouse.co.za">tian@solutionhouse.co.za</a></td>
<td><a href="http://www.solutionhouse.co.za">www.solutionhouse.co.za</a></td>
<td>34,35</td>
</tr>
<tr>
<td>Specialised Exhibitions</td>
<td>+27 (0)10 003 3077</td>
<td><a href="mailto:svenr@specialised.com">svenr@specialised.com</a></td>
<td><a href="http://www.securex.co.za">www.securex.co.za</a></td>
<td>39*</td>
</tr>
<tr>
<td>Sperons</td>
<td>0867 177 3767</td>
<td><a href="mailto:marihette.hattingh@spero.co.za">marihette.hattingh@spero.co.za</a></td>
<td><a href="http://www.spero.co.za">www.spero.co.za</a></td>
<td>49,55*</td>
</tr>
<tr>
<td>Suprema</td>
<td>+27 (0)11 784 3952</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>61*</td>
</tr>
<tr>
<td>Technoswitch</td>
<td>+27 (0)11 794 9144</td>
<td><a href="mailto:info@technoswitch.co.za">info@technoswitch.co.za</a></td>
<td><a href="http://www.technoswitch.co.za">www.technoswitch.co.za</a></td>
<td>53*,54</td>
</tr>
<tr>
<td>Techsec Security Services</td>
<td>+27 (0)12 654 5985</td>
<td><a href="mailto:neale@thelabsa.com">neale@thelabsa.com</a></td>
<td><a href="http://www.thelabsa.com">www.thelabsa.com</a></td>
<td>24,26</td>
</tr>
<tr>
<td>T/A The Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TeleEye (South Africa)</td>
<td>+27 (0)11 557 9200</td>
<td><a href="mailto:info@teleeye.co.za">info@teleeye.co.za</a></td>
<td><a href="http://www.teleeye.com">www.teleeye.com</a></td>
<td>9,76</td>
</tr>
<tr>
<td>Tyco Security Products</td>
<td>+27 (0)82 566 5274</td>
<td><a href="mailto:emallett@tycoimt.com">emallett@tycoimt.com</a></td>
<td><a href="http://www.tycosecurityproducts.com">www.tycosecurityproducts.com</a></td>
<td>73</td>
</tr>
<tr>
<td>UTC Fire &amp; Security</td>
<td>+27 (0)11 579 7300</td>
<td><a href="mailto:utcfs.ssa@fs.utc.com">utcfs.ssa@fs.utc.com</a></td>
<td><a href="http://www.utcfssecurityproducts.eu">www.utcfssecurityproducts.eu</a></td>
<td>50,51,56</td>
</tr>
<tr>
<td>VIVOTEK Inc.</td>
<td>+886 2 8245 5282</td>
<td><a href="mailto:pr@vivotec.com">pr@vivotec.com</a></td>
<td><a href="http://www.vivotec.com">www.vivotec.com</a></td>
<td>68</td>
</tr>
<tr>
<td>ZKTeco (SA)</td>
<td>+27 (0)12 259 1047</td>
<td><a href="mailto:sales@zkteco.co.za">sales@zkteco.co.za</a></td>
<td><a href="http://www.zkteco.co.za">www.zkteco.co.za</a></td>
<td>OFC*,18*, 19*,74</td>
</tr>
</tbody>
</table>

* Denotes advertiser

For more information on these and other suppliers please see www.hsbd.co.za
Niche Surveillance Products
FOR THE SECURITY SPECIALISTS

The Niche solutions from KEDACOM give your control room eyes and ears on the ground through our range of body worn cameras, mobile cameras and mobile NVR’s.

Body Worn Cameras
See what your forces on the ground see & make better decisions.

Mobile Cameras & Mobile NVRs
Capture the 360 degree scene from your vehicle onto your mobile NVR.

Niche Security Cameras
Zoom in up to 5km before your presence is felt.

Why Choose KEDACOM Products?

We focus on solutions and provide the products to solve the problem. Our approach ensures optimum, cost effective solutions. We also supply Bullet, Dome, PTZ, Laser PTZ & Box Cameras, NVRs & the VMS platform.

KEDACOM / Recognitive IP Video Solutions
Video Surveillance Business

AVAILABLE FROM OUR EXCLUSIVE DISTRIBUTORS